Analyse des Einflusses der Datenpreisgabe und der Informationskontrolle auf die Akzeptanz von vernetzten Diensten im Automobil

vom Fachbereich Maschinenbau

der Technischen Universität Darmstadt

zur

Erlangung des Grades eines Doktor philosophiae (Dr. phil.)

DISSERTATION

Vorgelegt von

Jonas Walter, M. Sc.

Aus Dieburg

Berichterstatter:	Prof. Dr.-Ing. Ralph Bruder, TU Darmstadt
Mitberichterstatterin:	Prof. Dr. phil. Martina Ziefle, RWTH Aachen

Tag der Einreichung:	06.10.2020
Tag der mündlichen Prüfung:	15.12.2020

Darmstadt 2020

Walter, Jonas: Analyse des Einflusses der Datenpreisgabe und der Informationskontrolle auf die Akzeptanz von vernetzten Diensten im Automobil

Darmstadt, Technische Universität Darmstadt,

Jahr der Veröffentlichung der Dissertation auf TUprints: 2021

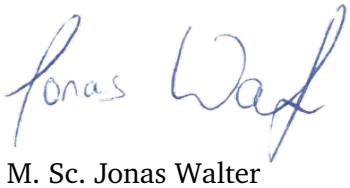
URN: urn:nbn:de:tuda-tuprints-178969

Tag der mündlichen Prüfung: 15. Dezember 2020

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit, abgesehen von den in ihr ausdrücklich genannten Hilfen, selbständig verfasst habe.

Darmstadt, 04.10.2020



M. Sc. Jonas Walter

Danksagung

An erster Stelle möchte ich meinem Doktorvater *Prof. Dr.-Ing. Ralph Bruder* danken. Durch die Möglichkeit, an Ihrem Institut zu promovieren, haben Sie den Grundstein für diese Arbeit gelegt. Zudem haben Sie mich über die komplette Promotionsphase hinweg immer wieder fachlich unterstützt und mich so auf meinem Weg begleitet. Ich danke Ihnen für die menschliche und fachliche Unterstützung. Für die Übernahme des Koreferats möchte ich mich bei *Prof. Dr.-phil. Martina Ziefle* herzlich bedanken.

Besonders möchte ich mich bei *Bettina Abendroth* bedanken. Deine fachliche, aber vor allem auch deine persönliche Führung haben es mir ermöglicht, auch unter gesundheitlich besonderen Bedingungen diese Arbeit anzufertigen. Dein Verständnis und deine Rücksicht schätze ich sehr und habe sie dabei niemals als selbstverständlich erlebt.

Dies gilt auch für das gesamte *IAD-Team*. Eure Kollegialität und Unterstützung werde ich sicherlich vermissen. Besonders eure kollektiven Video-Grüße, die mich im Krankenhaus erreicht haben, sind ein herausragendes Beispiel dafür. Einigen Kollegen und Freunde möchte ich besonders danken:

Pia, ich möchte dir als Kollegin und Freundin sehr für mehrere tolle, unterhaltsame, produktive und erlebnisreiche Jahre als Bürokollegen danken. Du warst immer eine ehrliche Sparrings-Partnerin, deren inhaltlichen Tiefe, Witz und Impulsivität ich sowohl privat als auch beruflich schätze. Genauso möchte ich auch dir, *Philip*, als Kollege und Freund danken. Deinen Ehrgeiz finde ich bewundernswert; für deine freundschaftlich-kümmernde Ader bin ich dir sehr dankbar. Außerdem möchte ich *Lukas Bier, Andreas Müller* und *Verena Klaer* als Kollegen und Sportspartner für den fachlichen Austausch, aber vor allem die gemeinsame Zeit bedanken.

Außerdem möchte ich mich bei allen Studierenden bedanken, die durch ihr Engagement im Zuge ihrer studentischen Arbeiten wesentlich zum Gelingen dieser Arbeit beigetragen haben. Auch den vielen Korrekturlesenden, die durch ihre Sorgfalt und Geduld geholfen haben, dieser Arbeit den letzten Schliff zu geben, gebührt ein herzlicher Dank.

Stellvertretend für viele weitere Freunde möchte ich *Klemens*, *Marius* und *Fari* danken, die schon seit lange vor dem Beginn meines Promotionsvorhabens immer als meine engsten Freunde für mich da sind. Es gibt so viel, für was ich euch danken möchte und hier nur als das gemeinsam Erlebte, die Freundschaft und die beständige Unterstützung beschreiben kann.

Den größten Dank möchte ich abschließend an meine Familie richten. An meine Eltern *Annedore* und *Heinz*, die mir mit bedingungsloser Liebe und Unterstützung alles das mit auf dem Weg gegeben haben, was mir diese Arbeit und noch viel mehr ermöglicht hat. Und an meine Geschwister *Felix* und *Sonja*, die immer eine Unterstützung sind. Ich danke euch sehr für den Halt und die verlässliche Stütze, die ihr gemeinsam für mich darstellt.

Zusammenfassung

Die Vernetzung von Verkehrsmitteln ist einer der zentralen Grundlagen zukünftiger Transportsysteme. So verspricht die Erfassung, Verarbeitung und der Austausch von Daten auch im Automobil ein Mehr an Sicherheit, Effizienz und Komfort. Obwohl Nutzende diesen Mehrwert wahrnehmen und schätzen, hegen sie gleichzeitig Privatheitsbedenken, die durch die vorhandenen Datenschutzpraktiken nicht ausreichend bedient werden. Vielmehr wünschen sich Nutzende ein Mehr an Transparenz und Kontrolle bezüglich der Datenpreisgabe. Während die Privatheit im vernetzten Automobil bisher vor allem aus technischer Perspektive betrachtet wurde, liegen bisher aus Nutzendensicht lediglich Befragungsstudien vor.

Daher ist ein Ziel dieser Arbeit modelltheoretisch zu klären, ob die Datenpreisgabe die Akzeptanz von vernetzten Diensten im Automobil beeinflusst und wie sich die Akzeptanz von vernetzten Diensten verändert, wenn eine selbstbestimmte Datenpreisgabe ermöglicht wird. Entsprechend wird in dieser Arbeit ein Akzeptanzmodell für vernetzte Dienste im Automobil unter Berücksichtigung privatheitsrelevanter Faktoren entwickelt und über drei Studien hinweg an je einem komfortbezogenen, effizienzbezogenen und sicherheitsbezogenen Dienst validiert. Für jede Studie wird in Anlehnung an bestehende Konzepte ein vernetzter Mehrwertdienst als Click-Dummy oder als animiertes Video visualisiert und zugänglich gemacht. Gleichzeitig wird in Studie 1 der Einfluss der tatsächlichen Informationskontrolle auf die Akzeptanz von vernetzten Diensten im Automobil beleuchtet.

Die Ergebnisse zeigen, dass privatheitsrelevante Faktoren über alle betrachteten Funktionsklassen hinweg einen signifikanten Einfluss zur Vorhersage der Nutzungsintention von vernetzten Mehrwertdiensten haben. Im Einklang mit der Kontextabhängigkeit des Konzepts der Privatheit variiert jedoch je nach Anwendungskontext die Rolle einzelner Faktoren wie das wahrgenommene Privatheitsrisiko oder das Vertrauen in den Anbieter eines vernetzten Dienstes. Weiterhin kann gezeigt werden, dass die Möglichkeit zu einer tatsächlichen Informationskontrolle zu einer signifikanten Senkung des wahrgenommenen Privatheitsrisikos sowie einer Verbesserung der Einstellung gegenüber der Nutzung eines vernetzten Dienstes führt. Eine signifikante Veränderung der Nutzungsintention von vernetzten Diensten im Automobil kann durch die Möglichkeit zu einer tatsächlichen Informationskontrolle jedoch nicht nachgewiesen werden.

Auf der Basis eines Vergleichs der unterschiedlichen Untersuchungskontexte der drei Studien wird ein Erklärungsansatz für die variierenden Rollen der betrachteten privatheitsrelevanten Faktoren entwickelt. Neben Implikationen für die Praxis werden abschließend detaillierte Untersuchungskonzepte für weitere Untersuchungen zur Rolle der informationellen Privatheit bei der Akzeptanz von vernetzten Diensten im Automobil abgeleitet.

Abstract

The connectivity of means of transport is among the major prerequisites of future transport systems. Accordingly, the introduction of data recording, data processing and data sharing promises an increase in safety, efficiency and comfort also in the automobile. Though users acknowledge this added value, they are concerned about their privacy which is not mitigated by existing privacy practices. Rather, users prefer practices of data disclosure which are more transparent and better controllable than the status quo. However, privacy in the connected vehicle has mainly been a topic from a technical point of view, whereas the user's view has only been covered by user surveys so far.

Therefore, the goal of this thesis to use a model-driven approach to clarify if aspects of data disclosure influence acceptance of connected services in the automobile. Moreover, it is elucidated if acceptance changes if a self-determined data disclosure is available. To do so, an acceptance model for connected services in the automobile which acknowledges privacy-relevant factors, is developed. Over three studies, the model is tested and validated against comfort-related, efficiency-related and safety-related connected services. Based on existing concepts of connected services, each services is visualized by either a custom-made animated video or an interactive click dummy. As the first study is carried out in a driving simulator, it is used to elucidate the influence of actual information control on the acceptance of connected services in the automobile.

The results reveal that privacy-relevant factors have a significant influence on the intention to use connected services in the automobile, irrespective of the functional category of the service. Congruent with the context dependency of the concept of privacy, however, the specific role of privacy-related factors varies with the context of use. If a self-determined privacy control is available, the perceived privacy risk decreases and the attitude towards using a connected service increases significantly. However, the availability of a self-determined privacy control does not affect the intention to use connected services significantly.

Comparing the different experimental settings across the three studies carried out in this thesis, an explanatory approach for the varying influences of specific privacy-related factors is deduced. Next to practical implications, suggestions for further experimental designs are made, which promote our understanding of the role that informational privacy plays in the acceptance of connected services in the automobile.

Abkürzungsverzeichnis

ACC	Adaptive Cruise Control
ATT	Einstellung gegenüber der Nutzung eines Systems *(engl.: Attitude towards using a system)*
AVE	Durchschnittlich erfasste Varianzen (*engl.: average variance extracted*)
BI	Nutzungsintention *(engl.: Behavioral intention to use a system)*
DSGVO	Datenschutzgrundverordnung
ECU	Elektronische Kontrolleinheit (*engl.: Electronic control unit*)
FAS	Fahrerassistenzsysteme
IC	Wahrgenommene Informationskontrolle (*engl.: perceived information control*)
IoT	Internet der Dinge (*engl.: Internet of Things*)
IT	Informationstechnologie
ITS	intelligente Transportsysteme
LBS	Standortbezogene Dienste (*engl.: location-based services*)
MICOM	Invarianz der Messmodelle (*engl.: Measurement invariance of composite models*)
NFC	Near Field Communication
PC	Privatheitsbedenken (*engl.: privacy concerns*)
PET	Privatheit steigernde Technologie (*engl.: Privacy-enhancing technology*)
PEOU	Wahrgenommene Einfachheit der Nutzung (*engl.: perceived ease of use*)
PLS	Partial least square – statistisches Verfahren für Regressionsmodelle
PR	Wahrgenommenes Privatheitsrisiko (*engl.: perceived privacy risk*)
PU	Wahrgenommene Nützlichkeit (*engl.: perceived usefulness*)
RALC	Theorie des beschränkten Zugriffs/der begrenzten Kontrolle
RSI	Relativer Geschwindigkeitsindex (*engl.: relative speed index*)
SN	Soziale Norm (*engl.: social norm*)
TAM	Technology Acceptance Model

TR	Vertrauen in den Anbieter (*engl.: Trust in the provider*)
UTAUT	Unified Theory of Acceptance and Use of Technology
V2I	Von einem Fahrzeug zur Infrastruktur (*engl.: Vehicle-to-infrastructure*)
V2V	Zwischen Fahrzeugen (*engl.: Inter-vehicle*)
V2X	Von einem Fahrzeug zu einer beliebigen Entität (*engl.: Vehicle-to-X*)
VANET	vehicular ad hoc Netzwerk
VDA	Verband der Automobilindustrie
VIN	Fahrzeugidentifikationsnummer (*engl.: Vehicle identification number*)

Inhaltsverzeichnis

1. Einleitung

Das Automobil ist immer noch das bevorzugte Fortbewegungsmittel der Deutschen (Bier et al., 2019). Dabei ist es vielmehr als nur ein Transportmittel um von A nach B zu kommen. Neben der Erfüllung von pragmatischen Funktionen weisen wir dem privaten Automobil auch eine affektive und symbolische Bedeutung zu (Steg, 2005). Die Fahrt mit dem privaten Automobil verbinden wir mit Stolz, Freiheit und Vergnügen. Personen bauen eine Beziehung zu ihren Automobilen auf, sodass eine emotionale Verbindung mit ihrem Automobil entsteht (Sheller, 2004). Diese Verbindung stützt und repräsentiert das Streben nach Sicherheit, Spaß und Unabhängigkeit, aber auch den Wunsch nach einem privaten Rückzugsort (Gardner & Abraham, 2007). Fragt man Pendler nach den Gründen ihrer Verkehrsmittelwahl, stößt man schnell auf die Vorzüge der Privatsphäre des Automobils (Ellaway et al., 2003). Aktuelle Automobile scheinen diesen Rückzugsort zu einer noch sichereren und komfortableren Umgebung zu machen. Durch den Einzug neuer digitaler Systeme, die in der Lage sind Informationen mit der Umgebung des Automobils auszutauschen, wird das Sicherheitsniveau im Automobil ebenso wie der gebotene Komfort deutlich erhöht. Darüber hinaus werden Tätigkeiten und Dienstleistungen, wie z. Bsp. der Zugriff auf das Internet und Streamingdienste im Automobil verfügbar, die man bisher nur über mobile Endgeräte erreichen konnte. Diese sogenannte Vernetzung hat einen hohen Stellenwert für die Automobilindustrie. Die Digitalisierung aktueller Automobile wird als alternativloser Schlüsseltrend betrachtet (Winkelhake, 2017). Trotz dieser Vorzüge und Fortschritte scheint der Einzug der Digitalisierung im Automobil in Konflikt mit dem Streben nach Privatheit zu stehen. Denn die digitale Transformation kommt nicht kostenlos, sondern basiert auf (nutzendenbezogenen) Daten. Um ihr Umfeld ebenso wie die Fahrerkabine überwachen zu können, sind Automobile mit einer Vielzahl von Sensoren ausgestattet (Huang et al., 2016). Angesichts dieser allgegenwärtigen Vernetzung gewinnt neben der physischen auch die informationelle Privatheit an Relevanz. War es bisher offensichtlich, ob man im Automobil physisch alleine und somit privat war, gilt diese Regel im vernetzten Automobil nicht mehr. Informationelle Privatheit scheint an einem Ort, der mit einer Vielzahl von Sensoren ausgestattet ist, die unter anderem auch das eigene Verhalten oder die eigenen Vitalfunktionen überprüfen, nur bedingt gegeben zu sein. Längst haben sowohl die Industrie (dpa, 2014) als auch die Forschung den Bedarf an privatheitswahrenden Lösungsansätzen erkannt und eine Vielzahl von technischen Möglichkeiten zur sicheren Datenverarbeitung aufgezeigt (z. Bsp. Hussain & Koushanfar, 2018). Gleichzeitig gewinnen digitale, datengetriebene Geschäftsmodelle einen immer höheren Stellenwert in der Automobilbranche. Die Umsatzprognosen für digitale Services im Automobil steigen stetig (Weber et al., 2019), während Automobilhersteller hohe Summen in die Vernetzung ihres Portfolios investieren (dpa, 2018).

Um mögliche Hürden neuer Produkte auf dem Markt vorherzusagen, werden Akzeptanzmodelle genutzt (Marangunić & Granić, 2015). Unterhalb dieses Sammelbegriffs für Theorien und Modelle zur Erklärung der Nutzungsintention einzelner Systeme verbergen sich Erklärungsversuche, welche Faktoren dazu beitragen, dass ein Produkt oder Service von der nutzenden Person angenommen oder abgelehnt wird. Auch für das Automobil existieren eine Vielzahl solcher Akzeptanzmodelle, die von spezifischen Assistenzsystemen (Park et al., 2015) über das automatisierte bis hin zum elektrischen Fahren reichen (Moons & Pelsmacker, 2012). Allerdings findet die Rolle der Privatheit im Zuge der Vernetzung des Automobils bisher in keinem dieser Modelle Berücksichtigung. Dabei zeigt der Blick in verwandte Kontexte, dass Nutzende eine mögliche Beschränkung ihrer Privatheit durch die Preisgabe von Daten sehr wohl für Nutzungsentscheidungen zu Rate ziehen (z. Bsp. Zhou, 2012). Nutzende hegen dabei ein Bedürfnis, Kontrolle über die preiszugebenden Daten ausüben zu können (Brell, Biermann et al., 2019), welches durch die existierende, unübersichtliche Datenschutzerklärung im Zuge der Unterschrift des Kaufvertrags nicht annähernd bedient wird (Akalu, 2018; Oltramari et al., 2018).

1.1. Ziele der Thesis

Um die bestehende Lücke an Akzeptanzmodellen, die den Aspekt der digitalen Vernetzung in Automobilen berücksichtigen, zu füllen, wird in dieser Arbeit ein Modell entwickelt, das die Wahrnehmung der Datenpreisgabe im vernetzten Automobil in klassische Akzeptanzmodelle integriert. Dabei wird das Modell am Beispiel von drei vernetzten Mehrwertdiensten im Automobil evaluiert und validiert. Da die Technologieakzeptanz stark mit dem jeweiligen Nutzungskontext variiert (Chesney, 2006), werden die drei Mehrwertdienste gezielt aus drei verschiedenen Kategorien von automobilen Mehrwertdiensten gewählt, sodass die bestehende Bandbreite an vernetzten Mehrwertdiensten im Automobil repräsentiert ist.

Untersuchungen zur Bereitschaft zur Datenpreisgabe aus anderen vernetzten Kontexten wie die Nutzung von sogenannten standortbezogene Dienste (LBS; Dienste, die zur Funktionsdarbietung positionsabhängige Daten nutzen) haben aufgezeigt, dass die Möglichkeit, Kontrolle über die Datenpreisgabe auszuüben, ein relevanter Faktor für die Nutzungsintention vernetzter Dienste sein kann (Hajli & Lin, 2016; Xu et al., 2013). Allerdings ist es bisher unklar, welche Auswirkung die Erfahrung einer tatsächlichen Kontrollmöglichkeit auf die Akzeptanz eines vernetzten Mehrwertdienstes im Auto hat. Daher wird in dieser Arbeit untersucht, ob und wie sich die Akzeptanz eines vernetzten Systems verändert, je nachdem, ob eine Möglichkeit zur selbstbestimmten Kontrolle der Datenpreisgabe gegeben ist.

Nicht im Fokus dieser Thesis steht der Wert, den Nutzende einzelnen Datentypen zuweisen. Hierzu gibt es bereits erste Ansätze zur Quantifizierung beziehungsweise Monetisierung der

subjektiven Bewertung von Datentypen (Acquisti et al., 2013; Danezis et al., 2005). Auch wenn der Kontext des vernetzten Automobils aufgespannt wird und einfache technische Architekturen eingeführt werden, liegt der Fokus dieser Thesis nicht auf technischen Lösungen weder zur Realisierung der Vernetzung im Fahrzeug, noch zur Sicherstellung einer privatheitswahrenden Kommunikation des Fahrzeugs mit anderen Entitäten. Ebenso wird in dieser Thesis keine juristische Expertise bezüglich der Wirksamkeit und der Geltungsspanne des Datenschutzrechts im vernetzten Automobil vorgenommen. Wiederum werden nur Grundzüge des Datenschutzrechts zur Verortung der Thesis im Themenkomplex herangezogen.

Zusammengefasst wird in dieser Arbeit untersucht, wie die Nutzungsintention von vernetzten Mehrwertdiensten im Automobil im Rahmen eines Akzeptanzmodells erklärt werden kann und ob dieses Modell für verschiedene Kategorien an Mehrwertdiensten Gültigkeit hat. Ein besonderer Fokus wird dabei auf die Beachtung der informationellen Privatheit durch die Nutzenden im vernetzten Auto gelegt. Darüber hinaus wird der Einfluss einer tatsächlichen, selbstbestimmten Kontrollmöglichkeit über die Datenpreisgabe auf die Akzeptanz von vernetzten Mehrwertdiensten im Automobil beleuchtet.

1.2. Aufbau der Thesis

In Kapitel 1 dieser Thesis wird das Thema eingeführt und motiviert. Die Ziele der Thesis werden abgegrenzt und die Struktur der Arbeit vorgestellt. Kapitel 2 bietet einen Überblick über den Stand der Forschung zu vernetzten Fahrzeugen, Datenschutz im Fahrzeug sowie der Akzeptanzforschung mit einem besonderen Fokus auf den automobilen Kontext sowie die Datenpreisgabe. Im Zuge dessen werden die notwendigen Kernbegriffe eingeführt und definiert. Kapitel 2 schließt mit der Ableitung der Forschungsfragen für diese Thesis. Kapitel 3 führt ein Akzeptanzmodell für vernetzte Dienste im Automobil ein und leitet die Hypothesen aus dem präsentierten Literaturüberblick ab. In Kapitel 4 werden drei Studien zur Evaluation und Validierung des Akzeptanzmodells präsentiert. Während Studie 1 im Fahrsimulator durchgeführt wurde, sind die Studien 2 und 3 online-basierte Replikationsstudien. In Kapitel 5 werden die Ergebnisse der einzelnen Studien zusammengefasst, verglichen und gegen den Hintergrund der bestehenden Literatur diskutiert. Abschließend bietet Kapitel 6 einen Ausblick mit Implikationen für Wissenschaft und Praxis.

2. Stand der Forschung

Auch wenn der Anteil von vernetzten Automobilen auf deutschen Straßen noch überschaubar ist (KBA, 2020; Statista, 2018), ist das vernetzte Automobil schon längst keine wissenschaftliche Neuentdeckung mehr. Unter Rückgriff auf bestehende Arbeiten wird in diesem Kapitel das Grundkonzept des vernetzten Automobils vorgestellt und eine Systematisierung für vernetzte Dienste im Fahrzeug eingeführt. Nachdem der Begriff der Privatheit im Allgemeinen beleuchtet wurde, wird die Rolle der Privatheit im vernetzten Automobil behandelt. Dabei steht der Stand der Forschung zur Nutzendenperspektive auf die Datenpreisgabe im vernetzten Automobil im Fokus. Darüber hinaus wird der Begriff der Akzeptanz sowie verwandter Konzepte eingeführt und die wichtigsten Akzeptanzmodelle kurz vorgestellt. Bestehende Akzeptanzmodelle für das Automobil einerseits sowie für vernetzte Anwendungen andererseits werden präsentiert. Abschließend werden die bisherigen Erkenntnisse zusammengefasst und die Forschungsfragen für diese Arbeit abgeleitet.

2.1. Das vernetzte Automobil

Obwohl bereits in den 1990er Jahren die ersten vernetzten Funktionen im Automobil Einzug hielten (Johanning & Mildner, 2015), hat sich bisher noch keine allgemein anerkannte Definition für ein vernetztes Automobil herausgebildet. In dieser Thesis wird auf die Definition von Coppola und Morisio (2016) zurückgegriffen, da sie sowohl die technische Infrastruktur als auch die funktionalen Merkmale vernetzter Automobile knapp beschreibt:

Ein vernetztes Automobil ist ein Fahrzeug, das durch festverbaute oder mitgebrachte Nutzergeräte fähig ist jederzeit auf das Internet zuzugreifen;

das mit modernen Anwendungen und dynamischen, kontextabhängigen Funktionen ausgestattet ist, sodass der fahrenden Person sowie den Passagieren fortgeschrittene Infotainmentfunktionen angeboten werden;

das in der Lage ist mit anderen intelligenten Geräten auf der Straße oder in Werkstätten zu interagieren, sodass es zum Ausbau einer Auto-zu-Infrastruktur-Kommunikationstechnologie beiträgt;

das fähig ist mit anderen Fahrzeugen zu interagieren, sodass es zur Etablierung von Fahrzeug-zu-Fahrzeug-Kommunikationstechnologien beiträgt. (Coppola & Morisio, 2016, S. 4)

Vernetzte Automobile sind mit einer Vielzahl kleiner Computer, sogenannter Electronic Control Units (ECUs), ausgestattet, die untereinander sowie mit weiteren Geräten innerhalb und außerhalb des Fahrzeugs verbunden sein können (Coppola & Morisio, 2016; Krauß & Waidner, 2015). Die dafür notwendige Systemarchitektur kann im vernetzten Automobil auf drei verschiedenen Arten vorliegen (Coppola & Morisio, 2016; Johanning & Mildner, 2015). In einem

embedded system verfügt das Steuersystem des Automobils über eine festverbaute Sim-Karte, sodass das vernetzte Automobil selbst als geschlossenes System eine dauerhafte Internetverbindung gewährleistet. Dem gegenüber steht das *integrated system*, bei dem die notwendigen Netzwerkkomponenten für den Zugriff auf das Internet durch integrierte, von dem Nutzenden mitgebrachte Geräte gestellt werden. Beispiele für *integrated systems* auf der Basis mobiler Endgeräte stellen Android Auto oder Apple CarPlay dar. Die dritte mögliche Systemarchitektur für vernetzte Automobile bewegt sich zwischen diesen beiden Polen. Das *tethered* bzw. *hybrid system* kann sowohl über festverbaute Elemente (wie z. Bsp. ein als Modem agierendes Steuergerät) als auch über integrierte Elemente verfügen (z. Bsp. Verbindung eines externen Geräts via Bluetooth). Um mit der Außenwelt drahtlos zu kommunizieren und einen Datenaustausch zu ermöglichen greifen vernetzte Automobile auf verschiedene Kommunikationstechnologien zurück. Diese umfassen *dedicated short range communication*, eine drahtlose Kommunikationstechnologie für kurze Entfernungen, die für den Einsatz im Automobil entworfen wurde; klassische Mobilfunkstandards wie *4G* und das aktuellere *5G*; lokale drahtlose Netzwerke wie *WiFi*, das auf den IEEE 802.11 Standards basiert; sowie innerhalb des Fahrzeugs *Bluetooth*-Netzwerke, die auf schwachen Radiowellen basieren und eine lokale Kommunikation ermöglichen und der Einsatz der *Near Field Communication (NFC)* Technologie, die einen Datenaustausch über eine Distanz von 4-10 cm ermöglicht (Dakroub et al., 2016). Durch den Einsatz dieser drahtlosen Kommunikationstechnologien wird der Austausch der Daten innerhalb des vernetzten Fahrzeugs (*intra-vehicle Kommunikation*) ebenso wie die Vernetzung des Automobils mit einer Vielzahl von externen Entitäten ermöglicht (*Vehicle-to-X Kommunikation, V2X*). Letztere lässt sich in drei verschiedene Anwendungsfälle unterscheiden (Berdigh & Yassini, 2017; Coppola & Morisio, 2016; Siegel et al., 2018). Der direkte Datenaustausch zwischen vernetzten Fahrzeugen wird als *inter-vehicle Konnektivität* (V2V) bezeichnet und ermöglicht eine schnelle Kommunikation und Orchestrierung mehrerer Fahrzeuge untereinander. Zusammen ergeben die kommunizierenden Fahrzeuge ein *vehicular ad hoc Netzwerk* (*VANET*). Der zweite Anwendungsfall ist die Kommunikation des vernetzten Automobils mit der umgebenden Infrastruktur. Bei dieser *vehicle to road infrastructure Kommunikation* (*V2I*) tauscht das vernetzte Automobil Daten mit intelligenten Elementen der Straßeninfrastruktur wie zum Beispiel vernetzten Ampelanlagen aus. Die Datenverbindung des vernetzten Automobils mit dem Internet (*Vehicle to Internet Kommunikation*) ermöglicht den Zugriff auf verschiedene Dienste aus dem vernetzten Automobil heraus und stellt eine Grundlage für die Auslagerung der notwendigen Rechenkapazitäten aus dem Automobil auf externe Server (im Kontext der Vernetzung auch als Verlagerung *in die Cloud* bezeichnet) dar. Basierend auf diesen Anwendungsfällen ermöglicht V2X in einer intelligenten Umgebung die Integration des einzelnen vernetzten Automobils in sogenannte

intelligente Transportsysteme (*ITS*). Diese umfassen nicht nur die Gesamtheit der vernetzten Fahrzeuge, sondern auch die intelligente Infrastruktur und sollen durch den Rückgriff auf moderne Kommunikationstechnologien die Gesamtheit des Transportsystems verbessern (Zhu et al., 2019).

2.1.1. Vernetzte Dienste im Automobil

Durch die oben beschriebene technische Infrastruktur entstehen im vernetzten Fahrzeug eine Vielzahl von Möglichkeiten für neue Anwendungen im Automobil, die weit über die Funktionen klassischer Fahrerassistenzsysteme (FAS) hinausgehen. Während FAS nach Winner et al. (2015) Informations- und Komfortsysteme umfassen, die den Fahrer bei Teilen der Fahrzeugführung unterstützen oder bei der Übernahme von Teilaufgaben entlasten, gehen sogenannte vernetzte Mehrwertdienste im Fahrzeug explizit über die Aufgaben der Fahrzeugführung hinaus. In Anlehnung an Reichwald et al. (2002) können vernetzte Mehrwertdienste im Automobil als Dienstleistungen definiert werden, deren Angebot und Funktion über den bereits bekannten Leistungsumfang von FAS hinausgehen und dabei mittels Internetzugriff und Telematik im Sinne der Vernetzung einen Mehrwert für den Nutzenden schaffen. Im Gegensatz zu FAS greifen vernetzte Mehrwertdienste auf die im vorangegangen Unterkapitel aufgezeigte vernetzte Infrastruktur zurück und tauschen Daten mit anderen Entitäten außerhalb der Systemgrenzen des eigenen Automobils aus. Martínez-Torres et al. (2013) haben am Beispiel von ITS 72 vernetzte Mehrwertdienste im Fahrzeug identifiziert und aufgezeigt, dass der Mehrwert der vernetzten Dienste für die nutzende Person in den Kategorien Sicherheit, Informationssysteme und ITS Management liegen kann. Darüber hinaus ergab eine Marktrecherche anhand der zehn umsatzstärksten Automobilhersteller 2018 41 verschiedene Mehrwertdienste im Automobil, die bereits auf dem Markt angeboten werden. Diese konnten in sieben Kategorien Kommunikation, Information, Navigation, Sicherheit & Wartung, Infrastruktur und Organisation eingeteilt werden (Walter et al., 2020). Ein Abgleich mit bestehenden Systematisierungsansätzen für vernetzte Mehrwertdienste (u. a. Bauer et al. (2006); Martínez-Torres et al. (2013)) mit solchen für FAS (u. a. Golias et al. (2002); Naab (2004); für einen vollständigen Überblick der betrachteten Systematisierungen siehe Walter et al. (2020)) ergab, dass keiner der betrachteten Kategorisierungsansätze in der Lage ist, die durch den Einzug von vernetzten Mehrwertdiensten erweiterte Servicevielfalt im vernetzten Automobil umfassend abzubilden. Daher wurde eigens für diese Arbeit ein neues Klassifikationssystem auf Basis der bestehenden vernetzten Mehrwertdienste am Markt als auch der existierenden Klassifikationsansätze für FAS und vernetzte Mehrwertdienste im Automobil abgeleitet. Unter Beteiligung mehrerer Experten für das automatisierte und vernetzte Fahren wurden über zwei Workshops hinweg die bestehenden Klassifikationsansätze bezüglich ihrer Eignung zur umfassenden Abbildung aller verfügbaren Dienste

im Automobil bewertet und ein neues Klassifikationssystem entwickelt. Tabelle 1 stellt das resultierende Klassifikationssystem dar. Die Ableitung kann in Walter et al. (2020) im Detail nachvollzogen werden. FAS und vernetzte Mehrwertdienste im Automobil werden in dem Klassifikationsansatz entsprechend der Ziele der Vernetzung des Automobils (Coppola & Morisio, 2016) in komfort-, sicherheits- und effizienzbezogene Dienste eingeteilt. Darüber hinaus werden die Dienste auf einer zweiten Ebene entsprechend des Objekts ihrer Einwirkung unterschieden (Fahrzeug vs. Fahrer). Damit erlaubt das Klassifikationssystem die Abbildung sowohl von FAS als auch vernetzter Mehrwertdienste im Automobil, ohne jedoch auf eine detaillierte Berücksichtigung der menschlichen Informationsverarbeitung oder den Fahraufgaben wie in Winner et al. (2015) oder Gründl (2005) zurückzugreifen.

Tabelle 1. Integrativer Klassifikationsansatz für Fahrerassistenzsysteme und vernetzte Mehrwertdienste im Automobil. Beispielhafte FAS und vernetzte Mehrwertdienste sind *kursiv* eingefügt. Darstellung nach Walter et al. (2020).

			Fahrerassistenz-systeme	**Vernetzte Mehrwertdienste**
Sicherheit	Fahrer	Fahrerinformation	*Gefahreninformationen*	
			Bordsensorik	*Ext. Informationen*
		Wahrnehmungsassistenz	*Verkehrszeichen-erkennung*	
		Fahrerbeobachtung	*Wachsamkeits-kontrolle*	*Automatischer Notruf*
	Fahrzeug	Fahrzeugkontrolle & -beobachtung	*Automatisches Bremssystem (ABS)*	*Fernwartung*
		Kollisionsvermeidung	*Adaptive Cruise Control (ACC)*	
Komfort	Fahrer	Navigation	*Navigationssystem*	
			Nicht in Echtzeit	*in Echtzeit*
		Information	*Point-of-Interest-Informationen*	
			Nicht in Echtzeit	*In Echtzeit*
		Kommunikation		*Kommunikations-dienste (z. Bsp. Messenger)*
		Unterhaltung		*Online-Media-Streaming*
		Infrastruktur		*WLAN-Hotspot*
		Organisation		*Kalender / Terminplanung*
Effizienz	Fahrer		*Effizienzassistent*	*Dynamische Routenführung*
	Fahrzeug		*Stop-and-go System*	

2.1.2. Daten im vernetzten Automobil

Daten stellen die Grundlage der Vernetzung dar. Daher werden Daten auch als das neue Öl des Automobils bezeichnet (Becker, 2017). Doch um welche Daten handelt es sich dabei? Der genaue Umfang und die Art der anfallenden Daten unterscheidet sich zwischen den Herstellern und je nach Ausstattung des jeweiligen vernetzten Automobils. Allerdings lassen sich Klassen typischerweise im vernetzten Automobil anfallender Daten identifizieren.

Hansen (2015) unterscheidet zwischen Daten über das Fahrzeug, Daten über Personen im Fahrzeug und Daten über die Umgebung des Fahrzeugs. Zu den Daten über das Fahrzeug zählen Identifikatoren der einzelnen Geräte wie ECUs oder des vernetzten Automobils selbst, Telematikdaten wie Standortdaten und Geschwindigkeit, Daten über den Betriebszustand des Fahrzeugs und seiner einzelnen Komponenten sowie, falls vorhanden, Daten des Unfallspeichers. Zu den Daten über Personen im Fahrzeug zählen Registrierungsdaten im Zuge der Erstellung eines Nutzendenprofils, Nutzungsdaten wie personalisierte Einstellungspräferenzen für die Sitze oder die Auswahl von Musik in Streamingdiensten, physiologische Daten zur Erfassung des Fahrendenzustands sowie Daten der Sprach- und Datenkommunikation, zu denen Textnachrichten, Kalendereinträge und Steuerungsbefehle zählen. Unter den Daten über die Umgebung des Fahrzeugs fasst Hansen sowohl alle auf das Fahrzeugumfeld gerichtete Sensordaten des Fahrzeugs, die mit anderen Fahrzeugen geteilt werden können, sowie Daten eines möglichen WLAN-Hotspots zusammen.

Krauß und Waidner (2015) nehmen eine ähnliche Klassifikation vor, indem sie zwischen Betriebsdaten, Daten für Komfortfunktionen, Fehler- und Wartungsdaten, Unfalldaten sowie von den Insassen eingebrachte Daten unterscheiden. Betriebsdaten umfassen dabei unter anderem die Motortemperatur, den Kraftstoffstand oder die aktuelle Geschwindigkeit. Zu Daten für Komfortfunktionen zählen Krauß und Waidner die Außentemperatur, Daten der Rückfahrkamera oder Daten des fahrendenspezifischen Nutzungsverhaltens wie das Lenk- und Schaltverhalten. Fehler- und Wartungsdaten umfassen Fehlercodes und Warnungen, die bei unsachgemäßer Nutzung oder defekten Teilen ausgegeben werden. Unfalldaten umfassen einen Zeitstempel des Unfallgeschehens sowie Daten des Fahrzeugzustands wie zum Beispiel die aktuelle Querbeschleunigung des Automobils. Abschließend ordnen die Autoren der Klasse der von den Insassen eingebrachten Daten Infotainment-Daten wie Nutzungspräferenzen sowie Daten zu Einstellung und Personalisierung des Automobils und der vorhandenen Dienste zu.

Neben diesen von der wissenschaftlichen Literatur eingebrachten Datenklassifikationen hat auch der Verband der Automobilindustrie (VDA) mit einer „Landkarte der Datenkategorien“

eine Klassifikation von Daten im vernetzten Automobil veröffentlicht (Verband der Automobilindustrie, 2014). Dabei unterscheidet der VDA zwischen Daten, bei denen die Zweckbindung durch ein Gesetzt geregelt wird (z. Bsp. Daten, die von dem e-Call System erfasst werden), Daten moderner Dienste (z. Bsp. prädiktive Diagnosedaten oder Bewegungsprofile), kundeneigene beziehungsweise vom Kunden eingebrachte Daten (z. Bsp. Infotainment- und Komforteinstellungen), im Fahrzeug erzeugte, dem Fahrenden angezeigte Kraftfahrzeug-Betriebswerte (z. Bsp. Füllstände oder der aktuelle Verbrauch), im Fahrzeug erzeugte aggregierte Fahrzeugdaten (z. Bsp. Durchschnittsverbrauch oder die Durchschnittsgeschwindigkeit) sowie im Fahrzeug erzeugte technische Daten (z. Bsp. Sensor- und Aktuatordaten). Die Datenklassifikation des VDA ist weniger an funktionalen Kriterien wie die obigen Klassifikationen ausgerichtet, sondern orientiert sich bei der Klassifikationsbildung stärker an rechtlichen Vorgaben.

Am Beispiel des Automobilherstellers BMW soll hier exemplarisch dargestellt werden, welche Daten konkret für Drittanbieter in einem vernetzten Automobil zugänglich sein können. Die folgende Datenauflistung ist dabei jedoch nicht gleichzusetzen mit der Gesamtheit aller in einem vernetzten BMW anfallenden Daten, da die folgende Auflistung nur solche Daten enthält, die BMW über seine firmeneigene Plattform CarData an Dritte preisgibt. Über sogenannte OBD-Dongles, die physisch im Auto angebracht werden müssen, können Dritte möglicherweise ohne den Umweg über die CarData- Plattform auf weitere Daten zugreifen. BMW unterscheidet grob zwischen folgenden Datenklassen: standortbezogene Navigationsdaten, Servicedaten, Nutzungsdaten, Daten spezifisch für ein elektrisches Fahrzeug, der statistische Fahrzeugstatus sowie eine Sammelkategorie, die umweltbezogene und regionsbezogene Daten ebenso wie Einstellungen beinhaltet. Abbildung 1 listet alle von BMW über CarData für berechtigte Unternehmen zugänglich gemachten Daten auf.

Wie die vorangegangenen Unterkapitel deutlich gemacht haben, spielt die Erfassung, Verarbeitung und Kommunikation einer Vielzahl von Daten eine zentrale Rolle im vernetzten Automobil im Allgemeinen sowie bei vernetzten Mehrwertdiensten im Speziellen. Damit gewinnt die Privatheit im Automobil eine neue, noch bedeutendere Rolle. Die folgenden Unterkapitel führen daher das Konzept der Privatheit ein (Kapitel 2.2) und zeigen die (neue) Rolle im vernetzten Automobil auf (Kapitel 2.3).

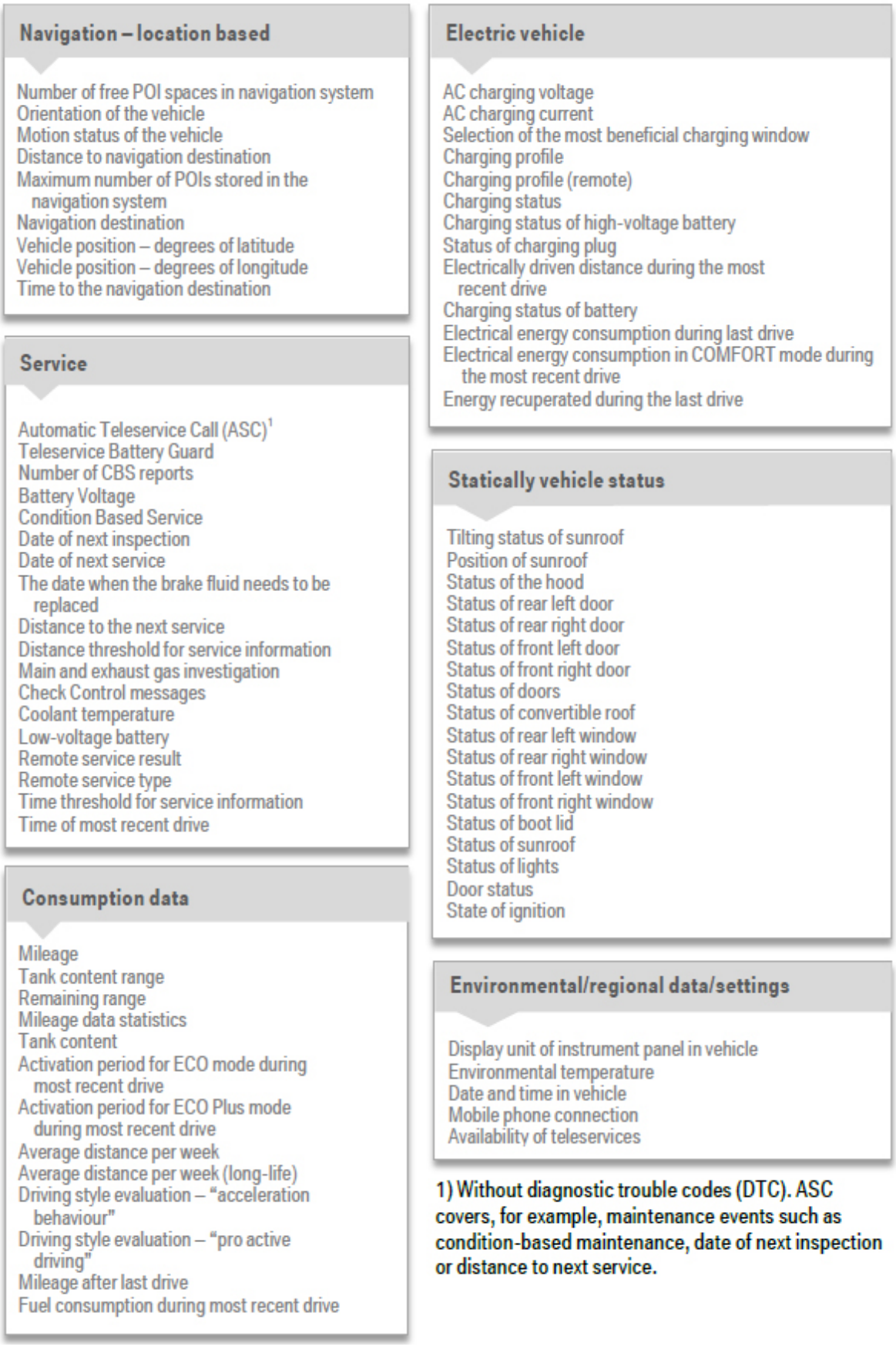


Abbildung 1. Übersicht über Daten, die durch Dritte über die Plattform BMW CarData abgerufen werden können. Entnommen aus BMW Group (2019).

2.2. Privatheit

Das Konzept der Privatheit erlebt im digitalen Zeitalter eine neue Hochphase, obwohl es weit über die digitalen Sphären hinausgeht. Bereits Ende des 19. Jahrhunderts definierten Warren und Brandeis (1890) Privatheit als das Recht alleine gelassen zu werden. Wie die folgenden weiteren Definitionsversuche zeigen werden, besteht trotz der langen Historie der interdisziplinären, wissenschaftlichen und gesellschaftlichen Diskussion um den Privatheitsbegriff keine allgemein anerkannte einheitliche Begriffsauffassung (Margulis, 2011). Vielmehr existieren verschiedene Definitionsversuche, die sich grob in Wert-basierte und auf artverwandte Begriffe beruhende Definitionen gliedern lassen (Smith et al., 2011). Darüber hinaus unterscheiden andere Definitionsversuche zwischen verschiedenen, spezifischen Arten der Privatheit (Tavani, 2008), aus denen sich auch der im Kontext dieser Arbeit besonders relevante Aspekt der informationellen Privatheit ableitet.

Wert-basierte Definitionen betrachten Privatheit als ein normatives, grundlegendes Recht oder beschreiben es, geprägt aus einer ökonomischen Perspektive, als Gut, mit dessen Preisgabe das Individuum angestrebte Vorteile erreichen kann (Smith et al., 2011). Letztere Perspektive ist auf den ökonomischen Prinzipien einer Kosten-Nutzen-Analyse gefußt und hat im Privatheitskontext mit dem privacy calculus Modell Einzug gehalten (Culnan & Armstrong, 1999; Dinev & Hart, 2006; Laufer & Wolfe, 1977). Das privacy calculus Modell beschreibt die Datenpreisgabe als das Resultat einer Abwägung zwischen erwarteten Vorteilen und antizipierten Privatheitsrisiken durch die Datenpreisgabe im Zuge der Nutzung eines Systems. Überwiegen die erwarteten Vorteile, so kommt es zur Datenpreisgabe (Dinev & Hart, 2006; Smith et al., 2011).

Artverwandte Definitionen (im Englischen *cognate-based definitions*) hingegen nehmen eine stärker kognitiv geprägte Perspektive ein und betrachten Privatheit als einen Zustand, der erwünscht oder unerwünscht sein kann und durch mehrere verschiedene Determinanten beeinflusst wird (Smith et al., 2011). Wichtig dabei ist der Einfluss der zeitlichen Dimension, die durch die Betrachtung der Privatheit als Zustand im Gegensatz zur normativen Auffassung der Privatheit als Grundrecht Berücksichtigung findet. Zurückliegende Erfahrungen, bestehende Erwartungshaltungen und veränderliche Umwelteinflüsse können demnach das angestrebte Ausmaß von Privatheit beeinflussen (Laufer & Wolfe, 1977; Smith et al., 2011; Westin, 2003). Westin (1967) definiert Privatheit „als Anspruch von Individuen, Gruppen oder Institutionen selbst zu entscheiden, wann, wie und in welchem Umfang Informationen über sie selbst anderen kommuniziert werden." (Westin, 1967, S. 7). Privatheit ist demnach ein dynamischer, zeitabhängiger Prozess und kann in verschiedenen Ausprägungen (zu hoch, angemessen, zu niedrig) vorliegen. Ebenso verstehen Laufer und Wolfe (1977) Privatheit als ein Konzept, das an konkrete Situationen gebunden und somit zeitvariant ist. Privatheit hat nach Laufer und Wolfe

drei Dimensionen: Selbst-Ego, umweltbezogen und interpersonell. Altman (1975) hingegen hebt den Aspekt der Kontrolle im Privatheitskonzept hervor, indem er Privatheit als „selektive Kontrolle des Zugriffs auf das Selbst definiert“ (Altman, 1975, S. 24). Die Kontrolle über die Privatheit ist für Altmann ein Prozess, der die Interaktion mit anderen reguliert und sowohl von internalen Zuständen des Regulierenden als auch von externen Umwelteinflüssen abhängt. Auch Margulis (1977) räumt der Kontrolle einen zentralen Aspekt im Konzept der Privatheit ein, in dem er Privatheit als „die Kontrolle über Transaktionen zwischen Personen und anderen“ definiert, „dessen ultimatives Ziel [es ist,] die Autonomie zu erhöhen und/oder die Verwundbarkeit zu reduzieren“ (Margulis, 1977, S. 10). Die Betrachtung der Kontrolle als zentrales Bestandteil des Privatheitskonzepts hat in der Folge Kritik erfahren (Margulis, 2003, 2011; Smith et al., 2011). Vielmehr wird die Kontrolle zwar als ein entscheidender, jedoch externer Faktor angesehen, der die Privatheit beeinflusst. Diese Sichtweise wird auch in dieser Arbeit eingenommen.

Das Verständnis des Konzepts der Privatheit hat sich in den letzten 100 Jahren stark mit dem Wandel von sozialen und politischen Strukturen, aber auch mit dem Fortschreiten der Technik verändert (Floridi, 2005; Smith et al., 2011; Westin, 2003). Während es initial vor allem als (physischer) Eingriff verstanden wurde, wurden Privatheitsbedenken später auch um Bedenken bezüglich der Interferenz mit der freien Entscheidungsfindung erweitert. Angesichts der fortschreitenden Vernetzung unseres alltäglichen Umfelds (Mai, 2016) dominiert heute die Sorge bezüglich des Zugriffs anderer auf die eigenen persönlichen Informationen (Shoemaker, 2010). Entsprechend unterscheidet Tavani (2008) zwischen vier verschiedenen Arten der Privatheit. Die *physische Privatheit* meint die Abwesenheit eines ungewollten physischen Eindringens, das durch den physischen Zugriff auf eine Person oder ihren Besitz gekennzeichnet ist. Die *entscheidungsbezogene Privatheit* hingegen bezieht sich auf die Freiheit von Interferenzen bei den eigenen persönlichen Entscheidungen und Plänen. Entscheidungsbezogene Privatheit liegt dann vor, wenn man Entscheidungen ohne die ungewollte Beeinflussung durch andere treffen kann. Als dritte Form liegt *psychologische Privatheit* vor, wenn man seine intimen Gedanken beschützen oder andere von dem Zugriff und der Manipulation seines Geistes abhalten kann. Als letzte Form der Privatheit liegt nach Tavani (2008) die *informationelle Privatheit* vor, wenn der Zugriff auf eigene persönliche Informationen kontrolliert und/oder eingeschränkt werden kann. Die betroffenen persönlichen Informationen können dabei ebenso bereits externalisiert in elektronischen oder digitalen Datenbanken vorliegen oder in persönlicher Kommunikation direkt ausgetauscht werden. Während frühere Theorien der informationellen Privatheit den beschränkten Zugriff anderer auf die eigenen persönlichen Informationen (*Theorie des beschränkten Zugriffs*)

(Allen, 1988; Bok, 1983) beziehungsweise die Fähigkeit der Kontrolle über die eigenen persönlichen Informationen (*Kontrolltheorie*) (Altman, 1975; Margulis, 1977) hervorheben, unternimmt die *Theorie des beschränkten Zugriffs/der begrenzten Kontrolle (RALC)* den Versuch beide Ansätze zusammenzuführen. Dabei unterscheidet die RALC (Tavani & Moor, 2001) zwischen dem Konzept der Privatheit und dem Management der Privatheit. So betont sie ebenso wie die Theorie des beschränkten Zugriffs die Relevanz der Fähigkeit eines Individuums den Zugriff anderer auf die eigenen persönlichen Informationen zu begrenzen. Gleichzeitig hebt sie die Signifikanz der Kontrolle für die Privatheit hervor, ohne jedoch die Kontrolle als Bestandteil des Privatheitskonzepts zu betrachten. Entsprechend hat man gemäß der RALC informationelle Privatheit in Situationen, in denen man vor dem Eindringen, der Interferenz oder dem Zugriff auf Informationen durch andere geschützt ist. Dieser Schutz kann durch die Beschränkung des Zugriffs anderer auf die persönlichen Informationen gewährleistet werden und wird durch die Fähigkeit zur begrenzten Kontrolle über den Informationsfluss ermöglicht. Der Wertschätzung dieser Konzeptualisierung unter anderem von Spinello (2015) folgend wird in dieser Arbeit die Definition von informationeller Privatheit nach Tavani und Moor (2001) übernommen.

2.3. Privatheit im vernetzten Automobil

Mit der Vernetzung hat auch die informationelle Privatheit endgültig Einzug in das Automobil gehalten. Waren bisher vor allem Aspekte der physischen Privatheit ausschlaggebend für die Wahl des Automobils als bevorzugtes Verkehrsmittel (Ellaway et al., 2003; Gardner & Abraham, 2007), rückt nun im Zuge der Vernetzung und der damit einhergehenden Datenerfassung, -übertragung, -sammlung und -auswertung auch die informationelle Privatheit in den Fokus (Lim & Taeihagh, 2018; Wachter, 2018). Neben einer Vielzahl neuer Geschäftsmodelle und neuer Umsatzpotentiale hat die Einbindung vernetzter Automobile in ITS entsprechend zu einem neuen Datenschutzbewusstsein in der Fahrzeugindustrie geführt. Dies spiegelt sich unter anderem in der Datenschutzvereinbarung des VDA wider, in der sich die deutsche Automobilindustrie zu den Grundsätzen der Transparenz, Selbstbestimmung und Datensicherheit bekennt (Verband der Automobilindustrie, 2014). Diese sind an die Datenschutzgrundverordnung (DSGVO) angelehnt, die seit dem 25. Mai 2018 in Kraft ist und die Verarbeitung personenbezogener Daten innerhalb der europäischen Union regelt. Ein zentraler Bestandteil der DSGVO ist die Formulierung von verpflichtenden Schutzzielen, die auch im vernetzten Automobil Anwendung finden (Wachter, 2018; Walter et al., 2018). Die Schutzziele sind in Tabelle 2 zusammengefasst.

Tabelle 2. Erläuterung der Schutzziele nach DSGVO (basierend auf Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (2019) und Bock und Meissner (2012))

Schutzziel nach DSGVO	**Erläuterung**
Datenminimierung	Es dürfen nicht mehr personenbezogene Daten erhoben, verarbeitet und genutzt werden, als das Erreichen des Verarbeitungszwecks erforderlich ist.
Verfügbarkeit	Die verarbeiteten Daten müssen für die berechtigten Personen zugreifbar sein. Es ist zu gewährleisten, dass personenbezogene Daten auffindbar und gegen zufällige Zerstörung oder Verlust geschützt sind
Integrität	Es muss sichergestellt werden, dass ein System genau so funktioniert, wie es funktionieren soll und personenbezogene Daten vollständig, aktuell und inhaltlich richtig sind.
Vertraulichkeit	Die unbefugte Kenntnisnahme von personenbezogenen Daten muss verhindert werden.
Nicht-Verkettbarkeit	Personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, dürfen nicht verkettet werden.
Transparenz	Die betroffene Person muss Kenntnis von den Datenverarbeitungsvorgängen haben. Die Verarbeitung von personenbezogenen Daten muss mit zumutbaren Aufwand nachvollzogen, überprüft und bewertet werden können.
Intervenierbarkeit	Die betroffenen Personen müssen jederzeit in der Lage sein, in die Datenverarbeitungsprozesse (korrigierend) eingreifen zu können. Dies schließt die Betroffenenrechte auf Widerspruch, Sperrung und Berichtigung ebenso wie Aufklärungs-, Auskunfts- und Löschungspflichten seitens der verantwortlichen Stellen mit ein.

In ihrer Gesamtheit verfolgen die Schutzziele den Zweck, das Grundrecht auf informationelle Selbstbestimmung umzusetzen. Die DSGVO und somit auch ihre Schutzziele kommen auch im vernetzten Automobil dann zu tragen, sobald Daten erfasst und/oder verarbeitet werden, die

personenbeziehbar sind. Diese Personenbeziehbarkeit kann durch einen eindeutigen Identifikator (zum Beispiel der Klarname der Nutzenden oder die Identifikationsnummer eines Automobils (*vehicle identification number; VIN*)) oder durch die Kombination von mehreren Daten, die in Isolation nicht personenbeziehbar sind, vorliegen (Akalu, 2018; Hansen, 2015; Wachter, 2018; Walter et al., 2018).

Besonders die Schutzziele der Transparenz und Intervenierbarkeit stellen die Angemessenheit der bisher gängigen Praxis unter anderem im Automobilsektor des Einholens einer einmaligen nutzerseitigen Einverständniserklärung mit Bezug auf die Datenschutzerklärung bereits beim Erwerb des Automobils in Frage (Akalu, 2018; Walter et al., 2018). Oltramari et al. (2018) fanden bei der Analyse von datenschutzbezogenen Einverständniserklärungen, dass 92 Prozent aller betrachteten Einverständniserklärungen zwar die Wahlfreiheit der Nutzenden beinhalten. Bei knapp der Hälfte der Einverständniserklärungen beschränkte sich diese Wahlfreiheit jedoch nur auf eine Alles-oder-Nichts-Wahl, die bei Widerspruch gegen die beschriebenen Datenschutzpraktiken die Nutzung des angebotenen Dienstes ausschließt. Entsprechend wurden die etablierten Datenschutzroutinen kritisiert und auf Basis der DSGVO Richtlinien und Verfahrensregeln formuliert, die die DSGVO-Schutzziele unter Rückgriff vor allem auf organisatorische Maßnahmen konkretisieren und erweitern. Wachter (2018) schlägt auf der Grundlage von ethischen und juristischen Bewertungen elf Designrichtlinien für vernetzte Geräte (wie zum Beispiel vernetzte Automobile) vor, die die transparente Kommunikation von Informationen über mögliche Datenschutzrisiken, transparente Verfahren zur Reduzierung der Gefahr der Profilbildung sowie transparente Vorgehensweisen im Falle eines Systemversagens mit Auswirkungen auf den Datenschutz der betroffenen Datensubjekte umfassen. Akalu (2018) fordert die Einführung von klaren Verfahrensregeln im Umgang von Daten, die im vernetzten Automobil erhoben und verarbeitet werden können, um den Schutz der informationellen Privatsphäre der Nutzenden gewährleisten zu können. So soll die nutzende Person in die Lage versetzt werden ihre Kontroll- und Entscheidungsrechte auch im Kontext des vernetzten Automobils umsetzen zu können. Erste Ansätze in diese Richtung sieht Akalu in Datenschutzvereinbarungen der Automobilhersteller wie die des Verband der Automobilindustrie (2014). Der Vorschlag für neue Verfahrensregeln zeigt beispielhaft, dass die Gewährleistung der Schutzziele technische und organisatorische Maßnahmen der datenerfassenden und –verarbeitenden Parteien erfordert. Während die von Akalu geforderten Verfahrensregeln vor allem organisatorische Aspekte aufgreifen, haben aus technischer Perspektive bereits umfangreiche Forschungsbemühungen stattgefunden, die eine privatheitswahrende und sichere Datenübertragung und –verarbeitung sicherstellen sollen. Im CONVERGE Projekt wurde ein privatheitswahrender Zugang zur Kommunikation mit ver-

netzten Automobilen entwickelt, der auf Pseudo- und Anonymisierungen der versendeten Daten basiert (Vogt et al., 2015). Das PRECIOSA Projekt stellte eine privatheitswahrende Architektur für kooperierende Systeme am Beispiel von vernetzten Automobilen vor und definierte im Zuge dessen technische Richtlinien für eine sichere und privatheitsbewusste Kooperation (Kung et al., 2011). Groll et al. (2009) stellten im Zuge des OVERSEE Projekts eine sichere Informationstechnologie-Plattform (IT-Plattform) für vernetzte Automobile vor, die zwischen vertrauenswürdigen und nicht vertrauenswürdigen Applikationen unterscheidet und den Zugriff auf die im Automobil anfallenden Daten kontrolliert. Seit 2014 existiert auch mit ISO 20078 eine Normreihe, die einen Standard für den Zugriff auf die im Automobil anfallenden Daten definiert und dabei Sicherheitsmechanismen für die Datenübertragung beinhaltet (ISO, 2019). Darüber hinaus wurden weitere technische Lösungsansätze vorgeschlagen, die unter anderem die privatheitswahrende Lokalisation von vernetzten Automobilen ohne den Rückgriff auf ein GPS-Signal ermöglichen (Hussain & Koushanfar, 2018), die Integration eines vernetzten, elektrischen Automobils in die Ladeinfrastruktur privat und sicher gestalten (Zhang et al., 2018) oder durch den Rückgriff auf weitere sogenannte privacy-enhancing technologies (PETs) die informationelle Privatheit im vernetzten Automobil allgemein schützen sollen (El-Rewini et al., 2020; Joy & Gerla, 2017; Karnouskos & Kerschbaum, 2018).

Während alle diese Ansätze eine sichere und privatheitswahrende Infrastruktur für das vernetzte Automobil zum Ziel haben, mangelt es ihnen jedoch an der Integration einer zentralen Sichtweise für den Datenschutz: die Nutzendenperspektive. Die nutzende Person des vernetzten Fahrzeugs als Datensubjekt im rechtlichen Sinne nimmt eine zentrale Rolle beim Schutz der Privatsphäre im vernetzten Automobil ein, da es um den Schutz der informationellen Privatheit eben dieser nutzenden Person geht. Ohne den Einbezug der Nutzendenperspektive auf vernetzte Automobile im Allgemeinen sowie einen möglichen Konflikt mit der informationellen Privatsphäre im Speziellen scheint eine angemessene Betrachtung der Problemstellung nicht möglich zu sein. Daher widmet sich das folgende Unterkapitel bisherigen Studien, die die Nutzendenperspektive auf das vernetzte Automobil beleuchtet haben.

2.3.1. Nutzendenperspektive auf vernetzte Automobile

Während die Vernetzung des Automobils eine Vielzahl neuer Funktionen wie zum Beispiel die oben eingeführten vernetzten Mehrwertdienste im Fahrzeug ermöglichen, erhöht sie gleichzeitig auch das Risiko einer Verletzung der informationellen Privatheit der nutzenden Personen. Wie wiegen Nutzende die Vorteile wie den Zugriff auf neue Funktionen gegen mögliche Nachteile wie einen Eingriff in die informationelle Privatheit ab? Welche Rolle spielt eine intakte informationelle Privatheit im vernetzten Automobil für die Nutzenden und welche Faktoren

werden von ihnen dabei als relevant betrachtet? Mit einem Blick auf bestehende Forschungsbeiträge zur Nutzendenperspektive auf vernetzte Automobile sollen im Folgenden diese Fragen erörtert werden.

Die Existenz vernetzter Automobile ist einem beträchtlichen Anteil der Nutzenden vor einer Teilnahme an einer entsprechenden Befragung inklusive Aufklärung nicht bewusst. Schoettle und Sivak (2014) sowie eine Studie der Unternehmensberatung Deloitte (2015) berichten eine geringe Kenntnis bezüglich vernetzter Automobile bei den Teilnehmenden der jeweiligen Umfragen. Aktuellere Studien zeichnen ein gemischtes Bild bezüglich des Bekanntheitsgrads vernetzter Automobile. In einem kleinem Interviewsample (N = 7) von Brell, Philipsen et al. (2019) war das Wissen über vernetzte Automobile durchweg verbreitet. Aufgrund der geringen Stichprobengröße kann diese jedoch auch durch die angewandte Rekrutierungsstrategie beeinflusst worden sein (z. Bsp. durch eine verstärkte Rekrutierung im Umfeld der Forschungsgruppe). In der gleichen Studie hatten jedoch Teilnehmer einer Onlinebefragung (N = 443) nur geringe Kenntnis von und Erfahrungen mit fortgeschrittenen Assistenzsystemen wie einem Notfallbremsassistenten, die von den Autoren als Stellvertretung für automatisierte und vernetzte Funktionen im Automobil genommen wurden. Liegt bei den Befragten nicht nur die Kenntnis, sondern bereits explizite Nutzungserfahrung durch den Besitz eines vernetzten Automobils vor, so hat dies direkten Einfluss auf die Art, wie das vernetzte Automobil wahrgenommen wird. In einer Studie von Svangren et al. (2017) beschrieben Nutzende von vernetzten Automobilen explizit als digitales Gerät anstatt als herkömmliches privates Fortbewegungsmittel. Die Digitalisierung und Vernetzung des Fahrzeugs prägt bei entsprechender Nutzungserfahrung dementsprechend das mentale Modell, dass die Nutzenden von ihrem Automobil aufbauen.

Nutzende erkennen die Vorteile, die mit der Vernetzung Einzug in das Automobil halten, an und schätzen die neue Funktionen. Dabei wird sicherheitsbezogenen Funktionen der höchste Stellenwert zugewiesen, gefolgt von effizienz- und komfortbezogenen Diensten (Brell, Biermann et al., 2019; Endo et al., 2016; Schmidt et al., 2016; Schoettle & Sivak, 2014; Shin et al., 2015). Walter und Abendroth (2018) konfrontierten in einer Online-Umfrage 101 potentielle Nutzende von vernetzten Automobilen mit verschiedenen Szenarien, in denen die Befragten entweder für sicherheits-, effizienz- oder komfortbezogenen Diensten Daten preisgeben mussten. Ähnlich wie Schmidt et al. (2016) fanden die Autoren, dass die Bereitschaft zur Datenpreisgabe und somit die Wertschätzung der angebotenen Funktion in den jeweiligen Szenarien für sicherheitsbezogene Dienste am höchsten war, gefolgt von komfort- und effizienzbezogenen Diensten. Dabei wird der wahrgenommene Nutzen von dem jeweiligen Nutzungskontext geprägt. Sahebi und Nassiri (2017) fanden darüber hinaus am Beispiel von nutzungsbasierten

Versicherungstarifen für das vernetzte Automobil, dass besonders risikoaverse Personen eine hohe Präferenz für sicherheitsrelevante Dienste haben. Befinden sich Personen alleine im Auto und haben somit keinen Mitfahrenden als Gesprächsteilnehmenden oder Assistenz, ist die Bereitschaft zur Datenpreisgabe für Infotainmentdienste im vernetzten Automobil höher als bei Personen mit Begleitpersonen (Endo et al., 2016). Darüber fand Eyssartier (2015) eine höhere Akzeptanz gegenüber des Einsatzes von Eventdatarekordern im Automobil bei einem professionellen Einsatz im Vergleich zum Einsatz im rein privat genutzten Fahrzeug. Vernetzte und automatisierte Technologien im Automobil werden von jungen potentiellen Nutzenden bereitwilliger akzeptiert als von älteren Personen (Bansal et al., 2016; Bansal & Kockelman, 2018; Owens et al., 2015), was aufgrund der höheren Liquidität älterer Personen die Frage nach der realistischen Erschwinglichkeit solcher Technologien für die interessierte Altersgruppe aufwirft.

Gleichzeitig sehen Nutzende in den Risiken für ihre informationelle Privatsphäre sowie der Sicherheit der technischen Infrastruktur vernetzter Automobile die größten Adoptionsbarrieren (Brell, Biermann et al., 2019; Schmidt et al., 2016; Schoettle & Sivak, 2014; Zmud et al., 2016). In einer Szenario basierten Online-Umfrage am Beispiel von vernetzten Infotainment- und Verkehrseffizienzdiensten mit 274 Teilnehmenden von Schmidt et al. (2017) bewerteten potentielle Nutzende vernetzter Automobile nur die Sicherheit des Fahrzeugs wichtiger als die Privatheit. Mögliche Vorteile der Vernetzung wie eine Erhöhung des Komforts, der Verkehrseffizienz oder monetäre Einsparungen wurden eine geringere Relevanz beigemessen als dem Schutz der eigenen informationellen Privatsphäre.

Im Zuge der Gestaltung der eigenen informationellen Privatsphäre variiert die Bereitschaft zur Datenpreisgabe mit dem Umfang und der Art der preiszugebenden Daten. Eriksson und Bjørnskau (2012) befragten 1319 Personen zu Privatheitsbedenken bei der Nutzung intelligenter Systeme zur Verkehrsüberwachung und –regulierung. Die Akzeptanz der Systeme sank mit zunehmendem Umfang der jeweils erfassten Daten.

Nicht nur der Umfang, sondern besonders auch die Art der preiszugebenden Daten beeinflusst die Bereitschaft zur Nutzung eines vernetzten Dienstes im Automobil. Je offensichtlicher die Personenbeziehbarkeit eines Datums, desto geringer die Bereitschaft der Nutzenden dieses preiszugeben (Brell, Biermann et al., 2019; Eyssartier, 2015; Schmidt et al., 2016; Walter & Abendroth, 2018). So fanden zum Beispiel Derikx et al. (2016) in einer Conjoint-Analyse zu pay-as-you-drive Tarifen für Kraftfahrzeugversicherungen, dass Verhaltensdaten bezüglich des eigenen Fahrverhaltens als kritischer und somit weniger teilbar wahrgenommen wurden als Positionsdaten des Automobils. Auch Schmidt et al. (2017) berichten eine geringe Bereitschaft personenbeziehbare Daten zu teilen. So waren Teilnehmende besonders bei demographischen,

psychophysiologischen und weiteren, direkt personenbeziehbaren Daten nicht bereit diese im Zuge der Nutzung eines vernetzten Automobils mit verschiedenen Entitäten zu teilen.

Neben dem Umfang und der Identität der preiszugebenden Daten beeinflussen auch die Identität sowie die Anzahl der empfangenden Entitäten die Bereitschaft zur Nutzung eines vernetzten Automobils. Während Nutzende die Preisgabe von Daten an öffentliche Autoritäten wie die Polizei, Rettungsdienste oder Institutionen des Verkehrsmanagements befürworten, wird die Weitergabe von Daten an private Akteure auf dem freien Markt abgelehnt (Brell, Philipsen et al., 2019; Schmidt et al., 2016; Schmidt et al., 2017; Walter & Abendroth, 2018). Doch auch innerhalb der privaten Datenempfänger unterscheidet sich die Bereitschaft der Nutzenden zur Datenpreisgabe. Im Kontext einer Fokusgruppenstudie zum Einsatz von Eventdatarecordern in privaten und professionellen Automobilen fand Eyssartier (2015), dass Nutzende zur Preisgabe von fahrzeug- und fahrverhaltensbezogenen Daten an den Fahrzeughersteller bereit sind, wenn dadurch potentiell die Fahrzeugsicherheit erhöht werden kann. Versicherungen als Datenempfänger wurden hingegen abgelehnt. Eine ähnliche Unterscheidung fanden auch Walter und Abendroth (2018), die zwar ebenfalls insgesamt eine geringe Bereitschaft zur Datenpreisgabe an private Marktteilnehmer berichteten, dabei jedoch eine höhere Bereitschaft zur Datenpreisgabe an Werkstätten und Automobilhersteller als an private Anbieter von fahrzeugbasierten Applikationen fanden. Derikx et al. (2016) hingegen berichten eine nutzendenseitige Bereitschaft zur Weitergabe der Daten an Versicherungen, wenn diese die primäre datenempfangende Partei darstellen. Die Datenweitergabe an Dritte (zum Beispiel für Marketingzwecke) wurde jedoch von den Teilnehmenden kategorisch abgelehnt.

Angesichts der vorhandenen Privatheitsbedenken und eines Bedürfnisses nach informationeller Privatheit im vernetzten Automobil fordern Nutzende eine erhöhte Transparenz bei der Erfassung, Kommunikation und Verarbeitung von Daten im vernetzten Automobil (Eriksson & Bjørnskau, 2012; Schmidt et al., 2016). In einer Studie zu automatisierten, vernetzten Fahrzeugflotten am Beispiel der Uber-Fahrzeugflotte fanden Bloom et al. (2017), dass die Datenerhebung im vernetzten Automobil akzeptiert wird, wenn deren Anlass und Rahmenbedingungen transparent gestaltet sind und die Nutzenden die Notwendigkeit der Datenerfassung nachvollziehen können. Ist der Grund für die Datenerfassung jedoch nicht ersichtlich, so sinkt die Akzeptanz der jeweiligen Technologie beziehungsweise des jeweiligen vernetzten Dienstes. Im Einklang mit der in Kapitel 2.3 aufgeführten Kritik an bestehenden Praktiken zum Einholen des Einverständnisses mit den geltenden Datenschutzerklärungen, sehen sich Nutzende nicht im Bilde, welche Daten im vernetzten Automobil zu welchem Zweck erhoben werden (Svangren et al., 2017). Vielmehr fordern sie mehr Informationen über die Datenerfassung ein, so zum Beispiel Informationen, wer welche Daten zu welchem Anlass erfasst (Brell, Biermann et al.,

2019). Eine transparente Kommunikation der Rahmenbedingungen der Datenerfassung erhöht die Wahrscheinlichkeit, dass ein vernetzter Dienst genutzt und Daten im Zuge dessen preisgegeben werden (Endo et al., 2016). Die Effektivität von Transparenz kann in dieser Hinsicht sogar finanzielle Anreize übertreffen (Walter & Abendroth, 2018).

Im Einklang mit der Forderung nach einer transparenteren Datenerfassung fordern Nutzende mehr Kontrollmöglichkeiten über die Datenpreisgabe im vernetzten Automobil ein (Brell, Biermann et al., 2019). In einer Befragungsstudie von Bloom et al. (2017) zeigten sich mehr als die Hälfte der Befragten bereit mehr als fünf Minuten aufzubringen, um die Erfassung von personenbeziehbaren Daten kontrollieren oder beenden zu können. Allerdings zeigt sich hier eine Kluft zwischen bekundeten Verhaltensintentionen und tatsächlichem Verhalten. Svangren et al. (2017) berichten in einer Interviewstudie mit frühen Nutzenden vernetzter Automobile, dass zwar ausgeprägte Privatheitsbedenken in Bezug auf die Preisgabe von personenbeziehbaren Daten im Zuge der Nutzung des elektrischen Automobils existieren. Keine der Interviewten hatte jedoch bereits versucht, Kontrolle über die Datenpreisgabe zu erlangen beziehungsweise die Datenpreisgabe zu unterbinden.

Während die Möglichkeiten der Vernetzung von Nutzenden somit wertgeschätzt werden, ist ihr Blick auf die Privatheit im vernetzten Automobil von Bedenken vor allem mit Bezug auf die Transparenz und Kontrolle über die Nutzung der preisgegebenen Daten geprägt. Das folgende Unterkapitel beleuchtet integrative Ansätze, die dem nutzendenseitigen Bedürfnis nach Kontrolle und Transparenz unter anderem im vernetzten Automobil gerecht zu werden versuchen.

2.3.2. Integrative Ansätze zur Wahrung der Privatheit im vernetzten Automobil

Die nutzendenseitige Forderung nach mehr Kontrolle und Transparenz bei der Erfassung und Verarbeitung von Daten steht im Einklang mit den Auflagen, die die DSGVO an die Erhebung personenbeziehbarer Daten stellt (siehe Tabelle 2). Daher existieren technische Lösungen, die die Schutzziele der DSGVO sowie den Privacy-by-Design Ansatz als Teil ihres Anforderungskatalogs betrachten, ohne dabei jedoch explizit auf die Nutzendensicht einzugehen (siehe zum Beispiel Dietzel et al. (2012)). Ohne eine umfassende Nutzendenevaluation bleibt es bei diesen Ansätzen jedoch unklar, ob sie den Anforderungen der Nutzenden tatsächlich genügen, obwohl sie deren privatheitsbezogenen Bedenken im vernetzten Automobil adressieren. Andere Ansätze aus dem Kontext vernetzter Geräte im sogenannten Internet of Things (IoT), zu dem auch das vernetzte Automobil gezählt werden kann, beziehen bestehende Nutzendenstudien bei der Anforderungsanalyse und Systemauslegung mit ein, mangeln jedoch ebenfalls an Nutzendenevaluationen (Carminati et al., 2016; Friginal et al., 2014; Oltramari et al., 2018; Sathyendra et

al., 2017; Wang et al., 2017). Diese Ansätze haben gemein, dass sie mittels technischer Lösungen die Privatheit der Nutzenden schützen und den Nutzenden im Zuge dessen Kontrolle über die Datenpreisgabe gewähren. Dabei bleibt jedoch unklar, wie diese nutzendenseitige Kontrolle genau ausgeübt werden kann und ob dies den Nutzenden auch gelingt. Im Folgenden sollen daher solche Ansätze im Fokus stehen, die explizit die Nutzendensicht bei der Entwicklung und Evaluation eines Systems zur Wahrung der Privatheit miteinbeziehen. Darüber hinaus wird mit CarData eine bereits existierende Datenplattform eines Automobilherstellers vorgestellt, die ebenfalls den Anspruch erhebt, Nutzende mit der Kontrolle über die Datenpreisgabe auszustatten.

2017 führte die BMW Group die Datenplattform CarData ein, die von allen Nutzenden von vernetzten Fahrzeugen der BMW Group genutzt werden kann (BMW Group, 2017). CarData dient dabei in der unternehmenseigenen Plattform für vernetzte Mehrwertdienste BMW ConnectedDrive als Zugangs- und Kontrollplattform. Während Nutzende die anfallenden Daten einsehen und für Drittanbieter im Zuge der Nutzung eines neuen Mehrwertdienstes freigeben können, ermöglicht CarData Dritten den Zugriff auf die anfallenden Daten, sofern eine nutzendenseitige Preisgabe vorliegt. Während CarData somit die Transparenz über die preiszugebenden Daten erhöht, ermöglicht die Plattform nur eine eingeschränkte Datenkontrolle. Zwar können Nutzende über die Datenpreisgabe an Dritte entscheiden, werden dabei jedoch weiterhin mit einer Alles-oder-Nichts-Entscheidung konfrontiert, die keine Entscheidung über die Preisgabe einzelner Datentypen erlaubt. Darüber hinaus beschränkt sich die Datenpreisgabe nur auf die Datenpreisgabe an Dritte. Bezüglich der Einschränkung der Datenübermittlung an die BMW Group schreibt diese in den FAQ auf ihrer Homepage: *„Derzeit ist es aus technischen Gründen nicht möglich, die Übertragung einzelner Telematikdaten selektiv zu aktivieren oder zu deaktivieren.“* (BMW Group, 2020). Plappert et al. (2017) kritisieren darüber hinaus, dass nicht zwischen datensparsamen und nicht datensparsamen Diensten unterschieden wird sowie dass die Informationsverarbeitung und -übertragung nicht durch PETs gesichert wird.

Einen Ansatz mit globaleren Wirkungsanspruch stellt das Databox Projekt dar, dass mit der Databox als physischen Gerät Nutzenden die Kontrolle über die Preisgabe von persönlichen Daten in einer IoT-Umgebung erleichtern soll (Crabtree et al., 2017). Dabei werden die Daten, die im Zuge der Nutzung von verschiedenen vernetzten Geräten und Services anfallen, lokal in der Databox aggregiert. Fragt ein Hersteller oder Serviceanbieter Daten zur Verarbeitung im Zuge der Nutzung seines Geräts oder Services an, erhält er Zugang zu den benötigten Daten in der Databox. Diese können dann lokal in der Databox verarbeitet werden.

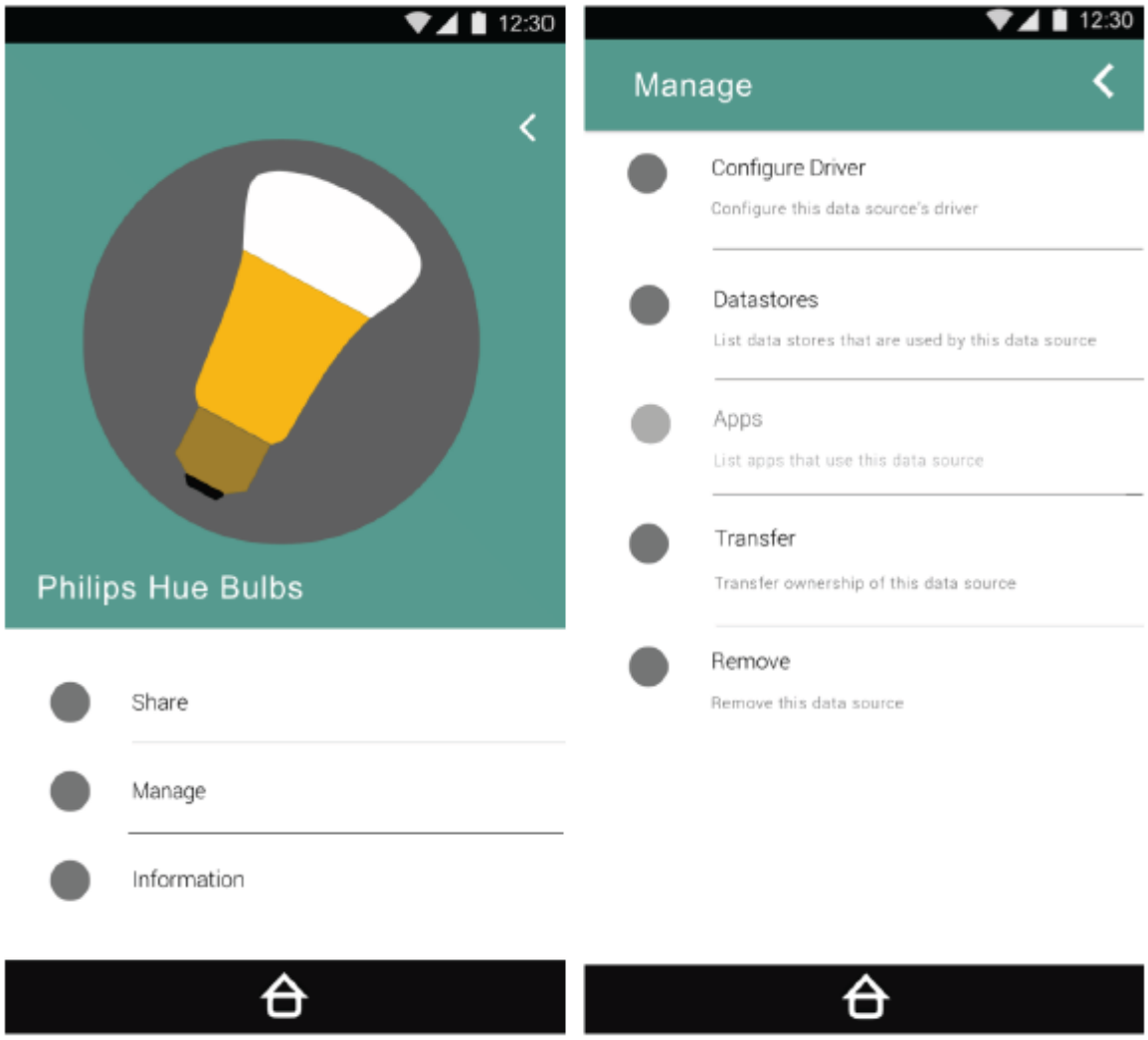


Abbildung 2. Screenshot der graphischen Oberfläche von Databox. Entnommen aus Crabtree et al. (2017).

Anstatt die Daten an Dritte zu senden, kontrolliert und managt die Databox den Zugriff auf Nutzendendaten, sodass nur die Verarbeitungsergebnisse auf Basis des beschränkten Datenzugriffs die Datenbox in Richtung des anfragenden Herstellers oder Serviceanbieter verlassen (McAuley et al., 2011). Neben der technischen Infrastruktur, die die lokale und sichere Datenverarbeitung in der Databox ermöglicht, wurde im Zuge des Forschungsprojekts eine nutzerfreundliche Schnittstelle zur Einsicht, Kontrolle und dem Management von persönlichen Daten angestrebt. Wie Abbildung 2 zeigt, können Nutzende über eine graphische Oberfläche auf die vorhandenen vernetzten Geräte zugreifen, um die angefallenen und genutzten Daten einzusehen oder Zugriffserlaubnisse zu erteilen. Über diese Schnittstelle können Nutzende auch auf sogenannte Manifeste zugreifen, die in einer einfach verständlichen Form Nutzenden vermitteln sollen, wer über welches Gerät Zugriff auf welche Daten erhalten möchte. Dem Nutzenden wird über die graphische Schnittstelle ermöglicht Vorteile und Risiken der Datenpreisgabe im Zuge der Nutzung eines Service oder Geräts abzuwägen sowie mittels granularer Wahlmöglichkeiten

die Preisgabe einzelner Datentypen zu kontrollieren. Damit gehen die im Databox Projekt erarbeiteten Kontrollmöglichkeiten über diejenigen der BMW CarData Plattform hinaus, laufen jedoch Gefahr, aufgrund ihrer Granularität die Bereitschaft und Fähigkeit der Nutzenden zur Wahrnehmung der gebotenen Kontrollmöglichkeiten zu überstrapazieren (Lin et al., 2014). Während sich die im Projekt primär verfolgten Anwendungsbeispiele im Smart Home Bereich befinden, ist das Databox-Konzept mit seinem globalen IoT-Anspruch auch auf das vernetzte Automobil anwendbar. Dabei steht die lokale Verarbeitung von Daten im Einklang mit Nutzendenpräferenzen, die das Verbleiben der Daten im eigenen Automobil bevorzugen (Brell, Biermann et al., 2019).

Das Datenmanagement für komplette IoT-Umgebungen unter Einbezug der nutzendenseitigen Kontrolle über die Datenpreisgabe hat auch das Projekt AVARE mit dem Kontrollsystem PRIVACY-AVARE zum Ziel (Alpers et al., 2017). PRIVACY-AVARE bietet dabei den Nutzenden die Möglichkeit über ein vernetztes Gerät ihrer Wahl Datenschutzeinstellungen vorzunehmen und in einem Datenschutzprofil zu speichern, das dann an alle verbundenen Geräte übertragen werden kann. Die Nutzenden können einerseits auf der Ebene einzelner Dienste die Datenpreisgabe regeln. Darüber hinaus kategorisiert PRIVACY-AVARE bestehende Dienste in funktionale Kategorien (z. Bsp. Navigation), für die vordefinierte Datenschutzeinstellungen vorgeschlagen und als Default gesetzt werden. Die Nutzenden können diese Datenschutzeinstellungen jederzeit ändern und werden dabei von PRIVACY-AVARE durch Datenschutzempfehlungen unterstützt. Dieser Ansatz ähnelt der Ableitung von Datenschutzprofilen für unterschiedliche Nutzendentypen, wie es bereits für Smartphone-Anwendungen demonstriert wurde (Liu et al., 2014). Der Einsatz vordefinierter Datenschutzeinstellungen ermöglicht den Nutzenden einen einfacheren und schnellen Zugang zur Datenschutzkontrolle, hält jedoch auch die Option von detaillierteren Datenschutzeinstellungen offen.

2.3.3. Die Datenschutzanwendung PRICON

Im Projekt SeDaFa (Selbstdatenschutz im vernetzten Fahrzeug) wurde mit der Datenschutzanwendung PRICON eine Datenschutzkontrollanwendung dezidiert für das vernetzte Automobil entwickelt (Walter et al., 2017). Unter Rückgriff auf PETs sowie im Einklang mit der DSGVO wurde dabei ein ähnlicher Mehrebenenansatz der nutzendenzentrierten Datenschutzkontrolle wie in dem AVARE-Projekt verfolgt (Plappert et al., 2017). Während eine technische Infrastruktur im Hintergrund mittels PETs die Datenschutzpräferenzen umsetzt, können Nutzende über ein Datenschutzdashboard Datenschutzeinstellungen global als auch auf der Ebene einzelner Dienste im vernetzten Automobil definieren.

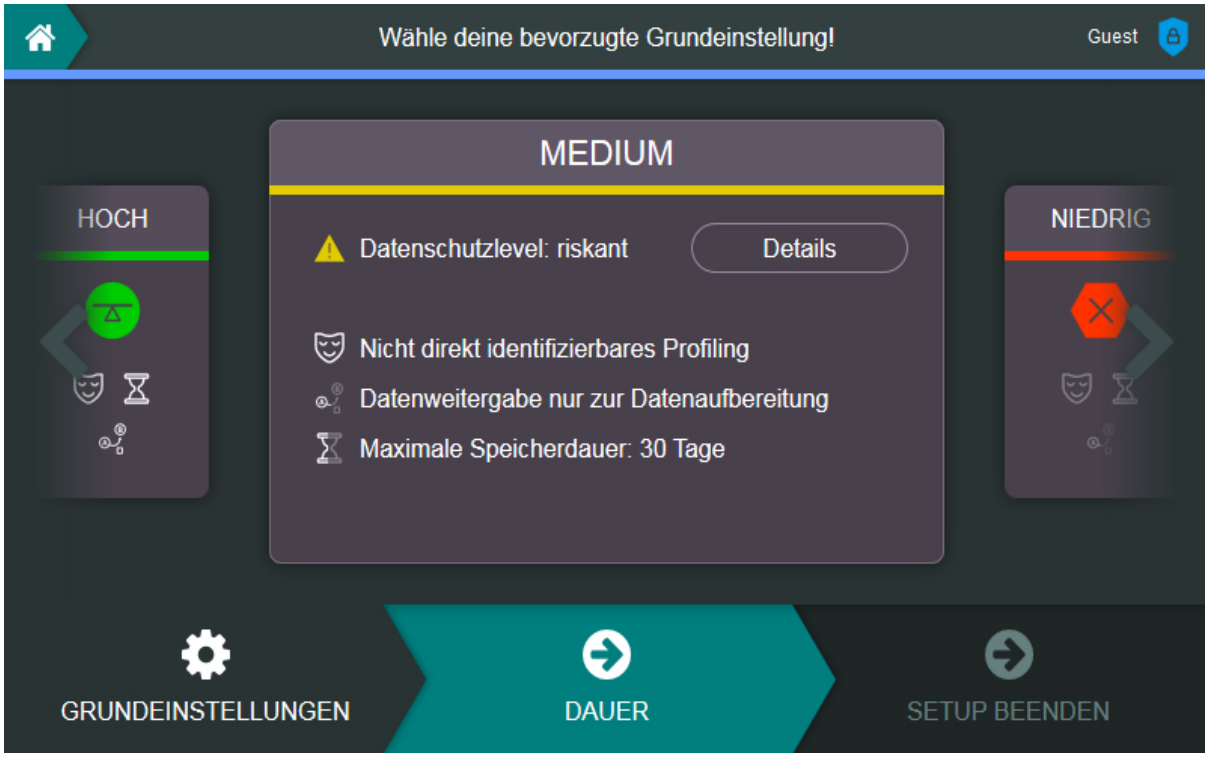


Abbildung 3. Screenshot der Datenschutzapplikation PRICON: Übersicht der vordefinierten Datenschutzprofile. Das vordefinierte Profil *Medium* ist ausgewählt.

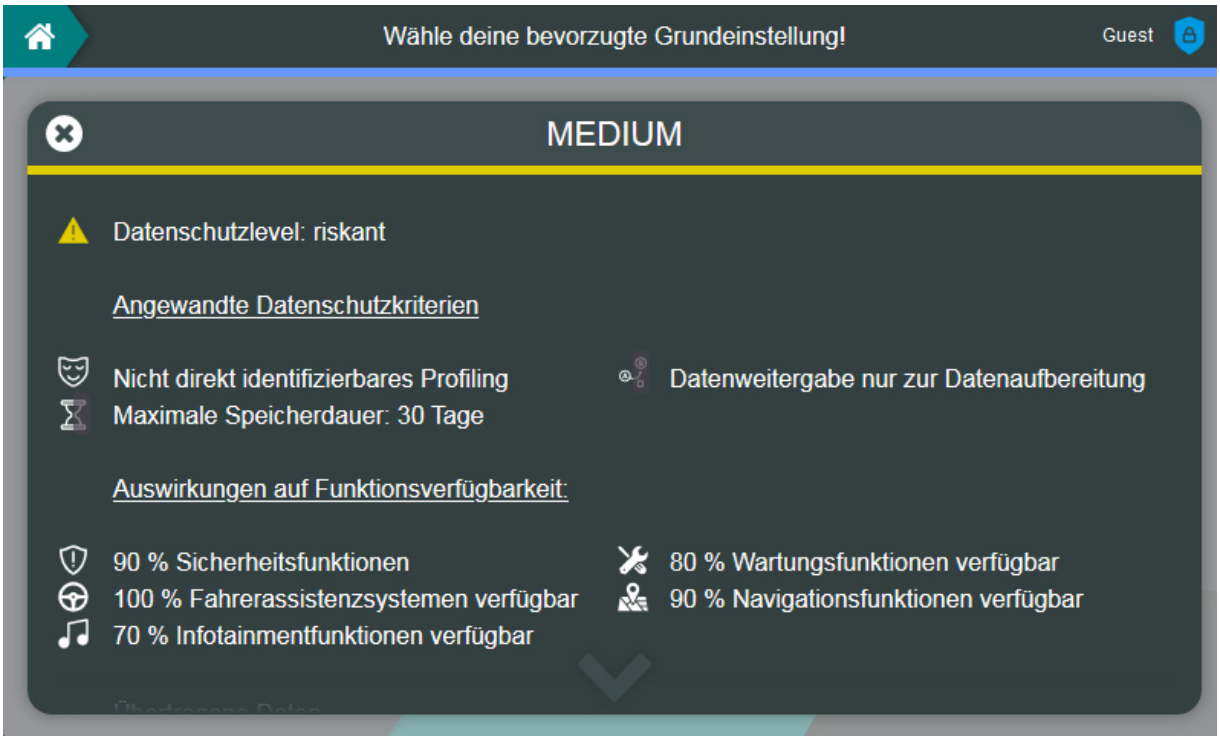


Abbildung 4. Screenshot der Datenschutzapplikation PRICON: Detailansicht des vordefinierten Datenschutzprofils *Medium*.

Unter der Berücksichtigung verschiedener Ausprägungen der Expertise der Nutzenden können Nutzende zwischen verschiedenen, vordefinierten Datenschutzprofilen (*Presets*) wählen oder eigene Datenschutzprofile erstellen, die jeweils global auf alle im vernetzten Automobil installierten Dienste angewendet werden. Als vordefinierte Presets stehen *Maximal, Hoch, Mittel* sowie *Niedrig* zur Verfügung, wobei *Maximal* nur die gesetzlich oder vertraglich vorgeschriebene Datenpreisgabe erlaubt, während *Niedrig* eine liberale Datenpreisgabe umsetzt. Wie die Abbildungen 3 und 4 zeigen, werden in der Übersicht der Datenschutzprofile die wichtigsten Eigenschaften mit einer Kombination aus Farbcodierung, Text und Icons transportiert (Abbildung 3), während interessierte Nutzende über eine Detailansicht weitere Informationen zu den Risiken und Konsequenzen der jeweiligen Datenschutzprofile einholen können (Abbildung 4).

Darüber hinaus besteht mit einer Personalisierungsfunktion auch die Möglichkeit ein Datenschutzprofil selbst zu definieren sowie im Zuge dessen Datenschutzeinstellungen für einzelne Dienste vorzunehmen (siehe Abbildung 5). Alle Datenschutzeinstellungen können in einem persönlichen Nutzendenprofil gespeichert werden, sodass die Datenschutzeinstellungen in allen Fahrzeugen, in denen PRICON verfügbar ist, aufgerufen werden können. Das Design von PRICON folgt explizit den Erkenntnissen aus Studien zur Nutzendensicht auf die Datenpreisgabe im vernetzten Automobil (siehe Kapitel 2.3.1).

Abbildung 5. Screenshot der Datenschutzapplikation PRICON: Datenschutzeinstellungen sind auch für einzelne Dienste möglich.

Die in den Detailansichten zur Verfügung gestellten Informationen entsprechen einerseits den juristischen und technischen Anforderungen, bieten dabei jedoch diejenigen Informationen zu solchen Kategorien dar, die von Nutzenden als besonders relevant erachtet wurden (z. Bsp. Nutzen eines vernetzten Dienstes oder preiszugebende Daten).

Das Layout der Einstellungen auf der Ebene einzelner Dienste (siehe Abbildung 5) orientiert sich an dem Privacy Calculus Modell (Dinev & Hart, 2006), in dem die Vorteile (Funktionen) und Kosten (preiszugebende Daten) in einer tabellarischen Ansicht direkt gegenübergestellt werden. Basierend auf der Annahme einer Kosten-Nutzen-Abwägung bei der Adoptionsentscheidung eines Dienstes unter der Preisgabe personenbeziehbarer Daten sollen die Nutzenden durch die Auswahl der dargebotenen Informationen sowie durch die graphische Aufbereitung bei einer informierten Datenschutzentscheidung unterstützt werden (Walter et al., 2017).

Die steigende Relevanz der informationellen Privatheit im vernetzten Automobil wurde, wie dieses Kapitel 2.3 zeigt, in juristischen und technischen Fachkreisen anerkannt. Gleichzeitig erkennen auch Nutzende die Bedeutung der informationellen Privatheit, fühlen sich jedoch durch die derzeit angebotenen gängigen Datenschutzpraktiken nicht ausreichend mit Kontrolle über die Datenpreisgabe ausgestattet. Erste integrative Ansätze, wie in diesem Subkapitel vorgestellt, schlagen neue Konzepte zur Unterstützung von selbstbestimmter Datenschutzkontrolle unter anderem im vernetzten Automobil vor, mangeln jedoch noch, mit der Ausnahme von BMW CarData, an dem Transfer von der Wissenschaft in die Praxis. Während die bisherigen Kapitel das vernetzte Automobil sowie die Rolle der Privatheit aus verschiedenen Perspektiven beleuchtet haben, steht eine modell-theoretische Betrachtung noch aus. Der Charme der modell-theoretischen Betrachtung liegt in dem Potential, Nutzendenverhalten nicht nur (retrospektiv) zu beschreiben, sondern darüber hinaus das beobachtbare Verhalten zu erklären und vorherzusagen. In dem folgenden Kapitel sollen daher zuerst theoretische Modelle für die Nutzung neuer Produkte im Allgemeinen und später für vernetzte Automobile im Speziellen betrachtet werden.

2.4. Modelle zur Beschreibung der Technologieakzeptanz und Technologieakzeptierbarkeit

Während die frühen, noch heute einflussreichen theoretischen Modelle allgemeines Verhalten beschreiben wollten, zielten mit dem Aufkommen erster persönlicher Rechner (PCs) ab den (späten) 1980er Jahren spätere Modelle gezielt auf den Einsatz und die Nutzung von zumeist technischen System oder Services ab. Allen Modellen gemein ist jedoch die grundlegende Annahme, dass Verhalten einerseits situations- und kontextspezifisch ist und anderseits nur durch

eine Aggregation mehrerer Faktoren, die sich in einer bestimmten Weise gegenseitig beeinflussen, zu beschreiben ist. In der Folge sollen die wichtigsten dieser Modelle in chronologischer Reihenfolge kurz vorgestellt werden. Zuerst werden jedoch die dafür zentralen Begriffe der *Technologieakzeptanz*, *Technologieakzeptierbarkeit* und *Technologieadoption* definiert und abgegrenzt.

2.4.1. Technologieakzeptanz, Technologieakzeptierbarkeit und Technologieadoption

Modelle zur Erklärung der Nutzung neuer Produkte oder Dienste beanspruchen für sich die Akzeptanz der im Fokus stehenden Technologien zu erklären. Bevor es hier zu einer Betrachtung der Modelle der Akzeptanzmodellierung kommt, scheint eine Betrachtung, Definition und Abtrennung der Begriffe *Technologieakzeptanz, Technologieakzeptierbarkeit* und *Technologieadoption* von Nöten zu sein. Obwohl dezidierte Modelle zur Erklärung der Nutzung neuer Produkte oder Dienste als Technologieakzeptanzmodelle bezeichnet werden, werden die Begriffe der Akzeptanz und Adoption oft austauschbar und ohne klare Definition verwendet (Nadal et al., 2019). Dies mag einerseits in dem Mangel eines einheitlichen Konsenses in der wissenschaftlichen Gemeinschaft bezüglich der Definition und Abgrenzung dieser Konstrukte begründet sein. Andererseits beanspruchen klassische Modelle zur Erklärung des Nutzungsverhaltens, wie sie in dem folgenden Kapitel vorgestellt werden, die Technologieakzeptanz und/oder –adoption zu erklären, ohne diese jedoch klar zu definieren (zum Beispiel Davis (1986)).

Renaud und van Blijon (2008) verstehen *Technologieadoption* als einen Prozess, der mit dem Aufmerksam werden des Nutzenden auf ein Produkt oder Service beginnt und mit der vollständigen Nutzung des Produkts oder Services durch den Nutzenden endet, sodass das Produkt oder der Service am Ende des Prozesses in den Alltag des Nutzenden integriert ist. *Technologieakzeptanz* verstehen die Autoren hingegen als wichtigen Schritt auf dem Weg zur vollständigen *Technologieadoption*, der als eine Einstellung des Nutzenden gegenüber der Technologie verstanden werden kann. Dieses Verständnis von *Technologieakzeptanz* als Einstellung gegenüber einer Technologie kann im Zuge einiger existierender Akzeptanzmodelle zu Problemen bei der Abgrenzung gegenüber relevanter Einflussfaktoren führen, da die Einstellung gegenüber der Nutzung eines Produkts bereits als wichtiger Einflussfaktor auf die Technologieakzeptanz beziehungsweise ihrer Operationalisierungen betrachtet wird. Abweichend von dem Verständnis Renaud und van Blijon (2008) von *Technologieakzeptanz*, aber integrierbar in deren Verständnis von *Technologieadoption*, unterscheiden Distler et al. (2018) sowie Martin et al. (2015) zwischen der Wahrnehmung eines Produkts oder Services vor der Nutzung (*Akzeptierbarkeit*) und der Wahrnehmung eines Produkts oder Services nach der Nutzung (*Akzeptanz*).

Technologieakzeptierbarkeit und *-akzeptanz* beschreiben somit die Produkt- oder Servicewahrnehmung eines Nutzenden zu verschiedenen Zeitpunkten innerhalb des Prozesses der *Technologieadoption*, deren Endstufe von keinen der beiden Konstrukte beschrieben wird. In einer Analyse der wissenschaftlichen Beiträge zu Technologieakzeptierbarkeit, -akzeptanz oder –adoption innerhalb des Gesundheitssektors fanden Nadal et al. (2019) jedoch, dass ein Großteil der betrachteten Studien entweder die zu untersuchenden Konstrukte wie Technologieakzeptanz nicht oder unzureichend definieren oder mit verwandten Konstrukten wie Technologieakzeptierbarkeit oder Technologieadoption verwechseln.

Diese definitorische Unklarheit resultiert womöglich auch aus dem Problem, dass keines der oben genannten Konstrukte direkt erfasst werden kann. Stattdessen werden beobachtbares Verhalten oder Verhaltensintentionen als Stellvertreter für die jeweiligen Konstrukte verwendet (Ando et al., 2016; Chen & Chen, 2009; Davis et al., 1989; Venkatesh et al., 2003). Folgt man den oben genannten Definitionen, so beschreibt das beobachtete Verhalten bei der (Nicht-) Nutzung eines Produkts oder Services die *Technologieakzeptanz*, während die Erfassung von Verhaltensintentionen sowohl die *Technologieakzeptanz* als auch die *Technologieakzeptierbarkeit* beschreiben kann. Der Zeitpunkt der Erfassung der Verhaltensintention relativ zum Zeitpunkt der Produktnutzung ist für die Abgrenzung der beiden Konstrukte entscheidend. Die Verhaltensintention beschreibt die *Technologieakzeptanz*, wenn sie nach einer tatsächlichen Interaktion der Nutzenden mit dem untersuchten Produkt oder Service erhoben werden. Hat eine solche Interaktion noch nicht stattgefunden (zum Beispiel im Falle von einer szenariobasierten Beschreibung des Produkts oder Services ohne reale Interaktionsanteile), zielt die Erfassung von Verhaltensintentionen auf die *Technologieakzeptierbarkeit* ab. Wie im weiteren Verlauf dieser Arbeit ersichtlich wird, werden in allen durchgeführten Studien die Verhaltensintentionen erfasst, dabei jedoch über die Studien hinweg sowohl die *Technologieakzeptierbarkeit* als auch die *Technologieakzeptanz* beschrieben

Trotz des Mangels einer einheitlichen, allgemein bekannten Abgrenzung der Konstrukte *Akzeptierbarkeit*, *Akzeptanz* und *Adoption* ist das allgemein als *Technologieakzeptanz* beschriebene Forschungsfeld innerhalb des kompletten IT-Sektors seit seiner Entstehung in den 1970er und 1980er Jahren sehr aktiv. Das nächste Kapitel gibt einen Überblick über diejenigen klassischen Modelle, die im Zuge dieser Arbeit von Relevanz sind.

2.4.2. Theory of Reasoned Action (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975)

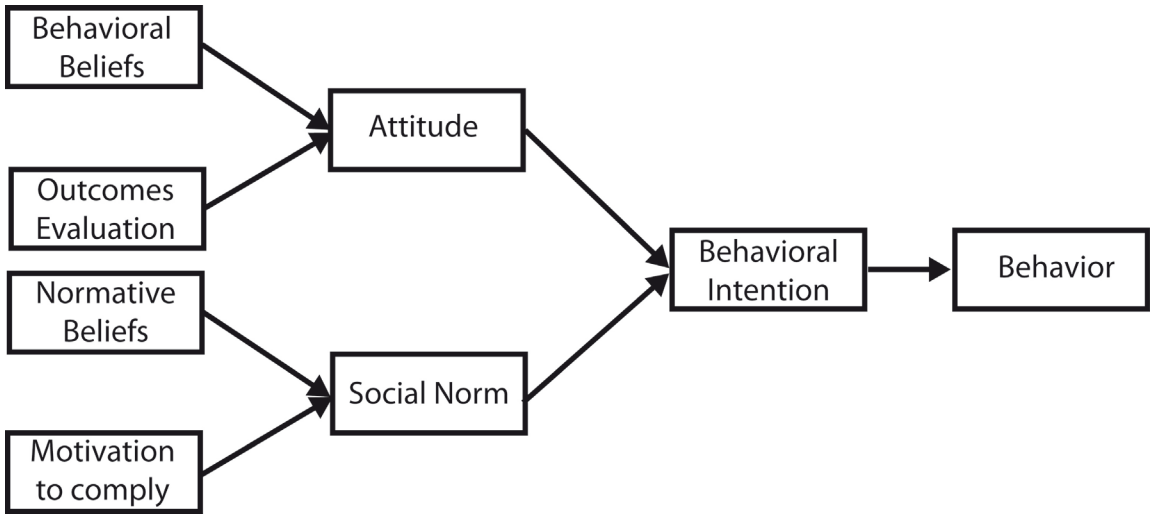


Abbildung 6. Theory of Reasoned Action nach Ajzen und Fishbein (1980). Eigene Darstellung.

Mit dem Anspruch menschliches Verhalten im Allgemeinen zu beschreiben formulierten Ajzen und Fishbein (1980) die *Theory of Reasoned Action*. Wie der Titel der Theorie bereits verrät, gehen die Autoren von einem rationalen Entscheidungs- und Abwägungsprozess aus, der dem menschlichen Verhalten zugrunde liegt. Dabei beschreiben sie diesen Prozess als eine Sequenz von Überzeugungen, Einstellungen, sozialen Normen und Verhaltensintentionen. Wie Abbildung 6 zeigt, stehen am Anfang von Ajzen und Fishbeins Theorie *verhaltensbezogene* und *normative Überzeugungen*. Die Überzeugung einer Person über die Konsequenzen der Ausführung eines bestimmten Verhaltens (*Behavioral Beliefs*) bilden gemeinsam mit der Bewertung dieser in Betracht gezogenen Konsequenzen (*Outcomes Evaluation*) die verhaltensbezogene Komponente. Die Überzeugung einer Person, wie andere Personen in ihrem Umfeld auf ein spezifisches Verhalten reagieren würden (*Normative Beliefs*), ergibt gemeinsam mit der Motivation einer Person, diesen wahrgenommenen normativen Erwartungen zu folgen (*Motivation to Comply*), die normative Komponente. Die *verhaltensbezogenen Überzeugungen* beeinflussen die *Einstellung* einer Person gegenüber der Ausführung des Verhaltens (*Attitude toward Behavior*), die als positive oder negative Bewertung des Verhaltens definiert ist. Die *normativen Überzeugungen* hingegen beeinflussen die *soziale Norm* (*Social Norm*), die als die Wahrnehmung einer Person wie Personen im sozialen Umfeld die Handlungsausführung bewerten würden definiert ist. *Einstellung* und *soziale Norm* beeinflussen wiederum die *Verhaltensintention* (*Behavioral Intention*), die als einziger direkter Prädiktor des betrachteten *Verhaltens* (*Behavior*) angesehen wird. Die

Autoren gehen davon aus, dass die relative Gewichtung des Einflusses von Einstellung und sozialer Norm auf die Verhaltensintention von dem spezifischen Verhalten, der Situation und interindividuellen Unterschieden beeinflusst wird (Ajzen & Fishbein, 1980).

Entsprechend ihres globalen Anspruches wurde die Theory of Reasoned Action in einem breiten Themenspektrum angewandt. Dazu gehören unter anderem das Essverhalten in Fastfood-Restaurants (Bagozzi et al., 2000), Managementstrategien (Myktytyn & Harrison, 1993) und moralisches Verhalten (Vallerand et al., 1992). Die Theory of Reasoned Action fand jedoch auch im Kontext von Informationssystemen (Mishra et al., 2014), Internetbanking (Nor et al., 2008), sozialen Netzwerken (Peslak et al., 2012) und IoT (Mital et al., 2018) Anwendung. Trotz ihrer breiten Anwendung erfuhr Ajzen und Fishbein's Theorie Kritik, unter anderem da die Ausführung eines bestimmten Verhaltens unter bestimmten Bedingungen trotz ausreichender Verhaltensintention nicht möglich erscheint (Ajzen, 1991; Sarver, 1983). Entsprechend formulierte Ajzen die *Theory of Planned Behavior*.

2.4.3. Theory of Planned Behavior (Ajzen, 1985)

Als eine Erweiterung der Theory of Reasoned Action unterscheidet sich die *Theory of Planned Behavior* nur von der vorangegangenen Theorie durch die Einführung des Konstrukts *wahrgenommene Verhaltenskontrolle (engl. Perceived behavioral control)*. Die wahrgenommene Verhaltenskontrolle kann als die wahrgenommene Kontrolle einer Person über interne und externe Faktoren, die relevant für die Ausführung eines spezifischen Verhaltens sind, betrachtet werden. Interne Faktoren sind zum Beispiel die Einschätzung eigener Fähigkeiten und Fertigkeiten sowie die Willensstärke. Externe Faktoren sind zum Beispiel die Möglichkeit zur Handlungsausführung, ausreichend Zeit, die Verfügbarkeit notwendiger Informationen sowie notwendige Ressourcen wie zum Beispiel Geld. Die *wahrgenommene Verhaltenskontrolle* ist dabei nicht gleichzusetzen mit der *tatsächlichen Verhaltenskontrolle*.

Während erstere, wie oben beschrieben, eine Wahrnehmung eigener Kontrollfähigkeiten auf Basis von interner und externer Faktoren beschreibt, umfasst letztere die bei der Handlungsausführung tatsächlich vorliegende Kontrolle einer Person über eine eigene geplante Handlung. Wie Abbildung 7 zeigt, sagt in der Theory of Planned Behavior die Verhaltensintention nicht mehr ein konkretes Verhalten, sondern den Versuch einer Verhaltensausführung vorher. Nur wenn eine ausreichende willentliche Kontrolle über das Verhalten vorliegt, kann das geplante Verhalten ausgeführt werden (Ajzen, 1985, 1991).

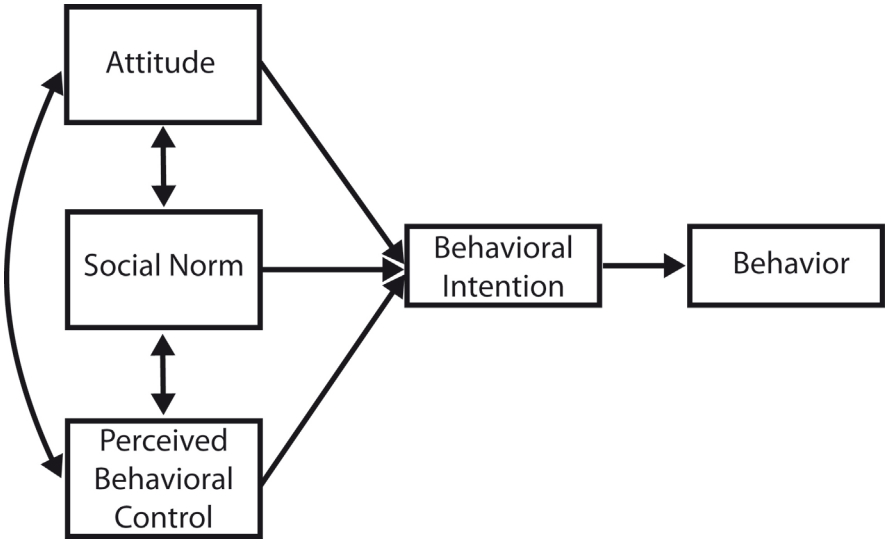


Abbildung 7. Theory of Planned Behavior nach Ajzen (1985, 1991). Eigene Darstellung.

Ebenfalls wie die Theory of Reasoned Action wurde auch die Theory of Planned Behavior für die Beschreibung eines breiten Spektrums von Verhalten angewendet (Ajzen & Driver, 1992; Askew et al., 2014; Beck & Ajzen, 1991; Gao et al., 2017; Godin & Kok, 1996; Oreg & Katz-Gerro, 2006; Pavlou & Fygenson, 2006; Yang et al., 2017). Entsprechend beansprucht auch die Theory of Planned Behavior menschliches Verhalten allgemein zu beschreiben. Diese Flexibilität kann als Vorteil, aber auch als Nachteil im Sinne von einer mangelnden Spezifizierung für bestimmte Kontexte ausgelegt werden. Daher wurden mit dem Aufkommen und der Verbreitung von PCs in der Arbeitswelt Modelle entwickelt, die den Anspruch haben Verhaltensintentionen und spezifische Verhalten im Kontext von IT-Systemen zu erklären.

2.4.4. Technology Acceptance Model (Davis, 1986)

Mit dem Einzug der IT in organisationale Strukturen nahm der Bedarf nach theoretischen Modellen, die die Nutzung oder Verweigerung von IT-Systemen erklären, zu (Lee, Y. et al., 2003). Im Zuge dessen entwickelte sich das Technology Acceptance Model (TAM; Davis, 1986) zu dem einflussreichsten Modell im IT-Sektor. Dabei ist der Anspruch des TAM die theoretisch validierte und sparsame Erklärung des Nutzungsverhalten von Computertechnologien (Davis, 1989; Davis et al., 1989). Um dies zu erreichen, nimmt das TAM Anleihen an der Theory of Reasoned Action (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975), in dem die Konstrukte *Einstellung gegenüber der Nutzung eines Systems (engl. Attitude towards using a system, ATT)* und *Nutzungsintention (engl. Intention to use a system, IU)* übernommen werden (siehe Abbildung 8). Die zentralen erklärenden Variablen im TAM sind jedoch zwei pragmatische Faktoren, die entweder die Nutzungsintention direkt oder vermittelt über die Einstellung gegenüber der Nutzung eines Systems beeinflussen.

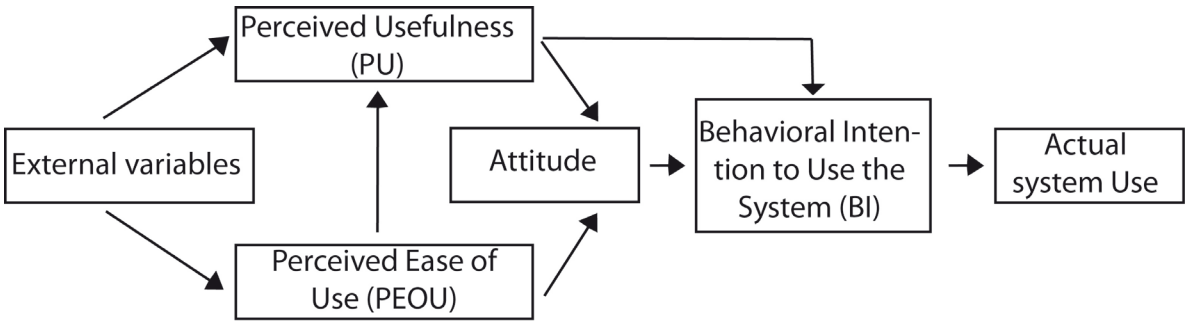


Abbildung 8. Technology Acceptance Model nach Davis (1986). Darstellung entnommen aus Walter und Abendroth (2020).

Die *wahrgenommene Nützlichkeit (engl. Perceived Usefulness, PU)* beschreibt das Ausmaß, in dem eine Person glaubt, dass ein bestimmtes System seine oder ihre Aufgabenerledigung unterstützen würde. Die *wahrgenommene Einfachheit der Nutzung (engl. Perceived Ease of Use, PEOU)* hingegen beschreibt das Ausmaß, in dem eine Person glaubt, dass ein bestimmtes System ohne mentalen oder physischen Aufwand zu nutzen ist.

In den letzten 34 Jahren wurden eine Vielzahl von Studien auf der Basis des TAM durchgeführt. Entsprechend des ursprünglichen Anwendungskontexts des TAM bewegen sich die meisten dieser Studien im IT-Sektor (Legris et al., 2003; Marangunić & Granić, 2015; Rokhiim et al., 2018). Während Davis ursprünglich für die Erfassung der Nutzung beziehungsweise Nutzungsintention von IT-Technologien im professionellen Kontext entwickelte, umfassen die bis 2020 vorliegende Studien auf der Basis des TAM ein deutlich breiteres Anwendungsspektrum, das häufig außerhalb des organisationalen Kontexts liegt. Hsiao und Yang (2011) identifizierten drei breite Anwendungskategorien des TAM: aufgabenbezogene Systeme, Onlinehandel und hedonische Systeme. Darüber hinaus fand das TAM auch intensiv Anwendung unter anderem in den Bereichen Erziehung und Lehre (Scherer et al., 2019), Pflege (Rahimi et al., 2018), soziale Medien (Wirtz & Göttel, 2016) und (mobiles) Online-Banking (Ahmad, 2018). Mit dem Aufkommen von ubiquitären und intelligenten Systemen hat sich auch der Einsatz des TAM in dem Kontext smarter Systeme vermehrt (Al-Momani et al., 2019; Bernsdorf et al., 2016; Boer et al., 2019; Müller-Seitz et al., 2009; Park, 2020).

Neben einer breitflächigen Anwendung in verschiedenen Kontexten erfuhr das TAM verschiedene Modellerweiterungen, von denen das TAM 2 (Venkatesh & Davis, 2000), das TAM 3 (Venkatesh & Bala, 2008) sowie die Unified Theory of Acceptance and Use of Technology (UTAUT, Venkatesh et al., 2003) die drei bekanntesten sind. Während das UTAUT im folgenden Abschnitt vorgestellt wird, werden das TAM 2 und TAM 3 hier kurz beschrieben. Das Modellerweiterung TAM 2 wurde mit der Motivation unternommen, die Determinanten von PU und IU

zu identifizieren. Dabei erweitert das TAM 2 das ursprüngliche TAM um folgende Variablen: *Freiwilligkeit, Erfahrung, Subjektive Norm, Image, Berufsrelevanz, Qualität des Ergebnisses und Demonstrierbarkeit des Ergebnisses*. Venkatesh und Bala (2008) fassten im TAM 3 die existierenden Forschungsergebnisse basierend auf dem TAM zusammen und ergänzten das TAM 2 um Determinanten, die auch die wahrgenommene Einfachheit der Nutzung erklären. Dabei wurde das TAM 2 um die folgenden Faktoren erweitert: *Selbstüberzeugung im Umgang mit Computern, Wahrnehmung externer Kontrolle, Angst gegenüber Computern, Verspieltheit im Umgang mit Computern, wahrgenommener Genuss* und *objektive Gebrauchstauglichkeit*.

2.4.5. Unified Theory of Acceptance and Use of Technology (Venkatesh et al., 2003)

Die Unified Theory of Acceptance and Use of Technology (UTAUT) stellt eine weitere Modellerweiterung des TAM dar. Im Gegensatz zum TAM 2 und 3 basiert die UTAUT dabei jedoch auf einer Analyse und Integration von acht verschiedenen Modellen zur Beschreibung der Nutzung eines (technischen) Systems, zu denen neben dem TAM auch die Theory of Reasoned Action und Theory of Planned Behavior gehören. Somit stellt das UTAUT den Versuch eines integrativen Ansatzes dar, der die einflussreichsten Modelle zum Zeitpunkt der Modellerstellung 2003 umfasst. Das UTAUT umfasst die Modellfaktoren *Leistungserwartung (engl. Performance expectancy), Aufwandserwartung (engl. Effort expectancy), sozialer Einfluss* (*Social influence*) und *erleichternde Bedingungen (engl. Facilitating conditions)*, die die *Nutzungsintention (engl. Behavioral intention)* oder im Fall der je nach Kontext neu zu spezifizierenden erleichternden Bedingungen das *Nutzungsverhalten (engl. Use behavior)* beeinflussen (s. Abbildung 9).

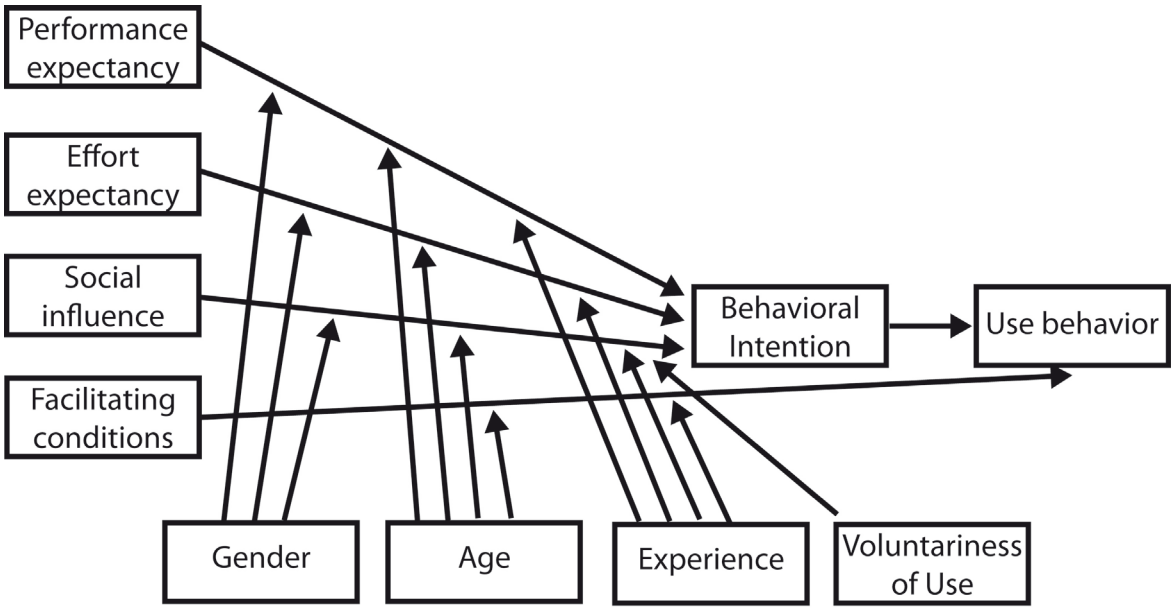


Abbildung 9. Unified Theory of Acceptance and Usage of Technology (Venkatesh et al., 2003). Eigene Darstellung.

Zusätzlich umfasst die UTAUT die Moderatorvariablen *Geschlecht (engl. Gender), Alter (engl. Age), Erfahrung (engl. Experience)* und *Freiwilligkeit der Nutzung (engl. Volutariness of use)*. Ähnlich wie das TAM wurde die UTAUT im organisationalen Kontext von den Autoren validiert, erfuhr seit seiner Veröffentlichung jedoch einen breiten Einsatz in verschiedenen Kontexten.

In einer Review identifizierten Williams et al. (2015) die Einsatzbereiche Kommunikationssysteme (z. Bsp. mobiles Banking, Instant Messaging, mobile Werbung), Systeme mit einem globalen Einsatzzweck (z. Bsp. Internet, Tablet-PCs, smarte Produkte, mobile Dienste), Bürosysteme (z. Bsp. Grafikprogramme, Referenzdatenbanken, Computer-basierte Assistenzsysteme) und spezialisierte Geschäftssysteme (z. Bsp. elektronische Personalmanagementsysteme, Weblog Technologien, biometrische Identifizierungssysteme). Dabei fand das UTAUT auch Einsatz im Kontext von IoT-Technologien (Al-Momani et al., 2019; Lee & Shin, 2019; Nysveen & Pedersen, 2016; Sung & Jo, 2018; Zhou, 2012).

2.5. Modelle für Technologieakzeptierbarkeit und Technologieakzeptanz im Automobil

Basierend auf den in Kapitel 2.5 eingeführten Modellen zur Beschreibung von Technologieakzeptierbarkeit und -akzeptanz wurden bereits mehrere Technologieakzeptierbarkeits- und Akzeptanzmodelle im Automobilkontext beschrieben.

Die Mehrheit der Veröffentlichungen griff dabei auf das TAM als Ausgangsmodell zurück (Berg, 2012; Buckley et al., 2018; Chen & Chen, 2009; Fazel, 2014; Ghazizadeh, Peng et al., 2012; Hegner et al., 2019; Keuntje & Poormohammadroohafza, 2014; Moták et al., 2017; Park et al., 2015; Payre et al., 2014; Simon et al., 2013; Sonneberg et al., 2019; Wu et al., 2019; Yoon & Cho, 2016), gefolgt von der Theory of Planned Behavior (Bamberg & Schmidt, 2003; Kelkel, 2015; Larue et al., 2015; Moons & Pelsmacker, 2012, 2015; Walsh et al., 2008) und der UTAUT (Madigan et al., 2016; Madigan et al., 2017; Osswald et al., 2012; Park et al., 2013). Lediglich eine Publikation griff primär auf die Theory of Reasoned Action zurück (Petschnig et al., 2014). Inhaltlich fokussierte sich die Mehrheit der Studien auf das automatisierte Fahren (N = 7), gefolgt von der Elektromobilität (N = 5) und dem vernetzten Fahren (N = 4). Den Fahrzeugassistenz- und Informationssystemen widmeten sich drei Studien. Zwei Studien entwickelten ein Modell zur Erklärung der Nutzungsintention für das Car Sharing, während je eine Studie die Nutzung des Automobils im Vergleich zu anderen Verkehrsmitteln und die Nutzung eines Mobiltelefons am Steuer untersuchte. Tabelle 3 fasst die inhaltliche Zuordnung der Arbeiten mit Entwicklung eines Modells zur Erklärung der Nutzungsintention oder Nutzung von Technologien im Automobilkontext zusammen.

Von den bestehenden Modellen zur Erfassung der Nutzungsintention oder Nutzung von vernetzten Technologien im automobilen Kontext untersuchten Larue et al. (2015) am Beispiel von intelligenten Bahnübergängen die Akzeptanz von ITS-Technologien, während Park et al. (2013) die Akzeptierbarkeit der Integration des Smartphones in das vernetzte Auto untersuchten. Die Autoren stellten eine stark abgewandelte Form des UTAUT auf, bei dem lediglich zwei Faktoren (erleichternde Bedingungen und Technographie / Offenheit für neue Technologien) signifikant zur Erklärung der Nutzungsintention beitrugen.

Yoon und Cho (2016) erweiterten das TAM um die Faktoren *Kompatibilität*, *visuelle Attraktivität, wahrgenommener Genuss* und *Aufgaben-Technologie-Passung*, um die Akzeptanz von vernetzten Diensten im Automobil zu erfassen. Dabei beschrieben die Autoren mehrere verschiedene vernetzte Dienste als Referenzstimuli, präsentierten jedoch gleichzeitig ein visuelles Interface eines nicht näher definierten vernetzten Dienstes. Aufgrund der Vorgabe mehrerer verschiedener Referenzstimuli scheint es möglich, dass unterschiedliche Teilnehmende sich auf unterschiedliche Dienste primär bezogen haben und somit unterschiedliche Bewertungsgrundlagen für das aufgestellte Modell herzangezogen haben. Dennoch ist die Stärke des Modells die stärkere Einbindung von affektiven Faktoren in das TAM, das für einen zu starken Fokus auf eine kognitive beziehungsweise instrumentale Bewertung von Systemen kritisiert wurde (Mahlke, 2005; van der Heijden, 2003).

Osswald et al. (2012) entwickelten das *Car Acceptance Model* (*CTAM*) als theoretisches Modell zur Erfassung der Akzeptierbarkeit und Akzeptanz von Informationssystemen im Automobil. Die Autoren erweiterten die UTAUT um die Faktoren *Angst (im Fahrzeugkontext)*, *Selbsteffizienz*, *Einstellung gegenüber der Nutzung der Technologie* und *wahrgenommene Sicherheit*. Allerdings wurde das CTAM nicht selbst evaluiert, sondern nur dem CTAM zugrundeliegende Fragebogen mit 21 Teilnehmenden an einem Texteingabeinterface im Automobil validiert.

Chen und Chen (2009) untersuchten die Akzeptierbarkeit von Telematik im Automobil anhand einer Erweiterung des TAM um die Faktoren *Soziale Norm* und *Wahrgenommene Verhaltenskontrolle* aus der Theory of Planned Behavior. Interessanterweise erklärte die Theory of Planned Behavior einen größeren Teil der Varianz der Nutzungsintention für den nicht näher spezifizierten Telematikdienst im Automobil als das von Chen und Chen entwickelte Modell, in dem *Soziale Norm* kein signifikanter Prädiktor der Nutzungsintention war.

Tabelle 3. Kategorisierung bisheriger Studien mit Modellen zur Erklärung der Nutzungsintention oder Nutzung von Technologien im Automobilkontext nach thematischen Kontext und primären Basismodell*.

Thema	TAM	TPB	TRA	UTAUT
Automatisierung	Buckley et al. (2018); Hegner et al. (2019); Moták et al. (2017); Payre et al. (2014)	Kelkel (2015)		Madigan et al. (2017); Madigan et al. (2016)
Elektromobilität	Fazel (2014); Wu et al. (2019)	Moons und Pelsmacker (2012); Moons und Pelsmacker (2015)	Petschnig et al. (2014)	
Fahrerassistenz- und Informationssysteme	Ghazizadeh et al. (2012); Park et al. (2015)			Osswald et al. (2012)
Vernetztes Fahren	Chen und Chen (2009); Yoon und Cho (2016)	Larue et al. (2015)		Park et al. (2013)
Car Sharing	Simon et al. (2013); Sonneberg et al. (2019)			
Nutzung des Automobils		Bamberg und Schmidt (2003)		
Nutzung des Mobiltelefons am Steuer		Walsh et al. (2008)		

* Einige Studien basieren auf mehreren Basismodellen. Um eine klare Kategorisierung zu ermöglichen wurden solche Studien zu dem Basismodell zugeordnet, dass in der jeweiligen Studie den größeren Einfluss hatte.

Trotz aller verschiedenen modelltheoretischen Ansätzen und Anwendungsszenarien der bisher bestehenden Modelle zur Erklärung der Akzeptierbarkeit und Akzeptanz von vernetzten Systemen im automobilen Kontext teilen alle gemeinsam eine Eigenschaft: Obwohl alle den Anspruch erheben vernetzte Dienste im Automobil oder in dessen Umfeld zu erfassen, geht keines der Modelle auf den Aspekt der Datenpreisgabe und die damit verbundenen Privatheitsbedenken der Nutzenden (siehe Kapitel 2.3.1) ein. Da es im automobilen Kontext noch an modelltheoretischen Ansätzen unter Einbezug privatheitsrelevanter Faktoren mangelt, wirft das folgende Kapitel einen Blick auf bestehende Modelle zur Erklärung der Datenpreisgabe in datenintensiven Kontexten außerhalb klassischer Internetanwendungen.

2.6. Modelltheoretische Ansätze zur Erklärung der Datenpreisgabe in datenintensiven Kontexten

Die Vernetzung des Automobils geht einher mit einem geringen nutzendenseitigen Bewusstsein für die Integration des Fahrzeugs in das Internet (Deloitte, 2015; Schoettle & Sivak, 2014). Diesen Umstand teilt das vernetzte Automobil mit weiteren (Alltags-)Geräten im IoT, die durch die Integration von Computern internetfähig werden, ohne dass sie als Computer wahrgenommen werden (Tene & Polonetsky, 2013). Karaboga et al. (2015) sprechen daher im IoT-Kontext (zudem auch das vernetzte Automobil gezählt wird) von einem "versteckten Internet". Aufgrund dieser Ähnlichkeit von vernetzten Automobilen und anderen vernetzten Geräten im IoT mit Bezug auf das mangelnde nutzendenseitige Bewusstsein für die Konnektivität wird in diesem Kapitel ein Blick auf ausgewählte modelltheoretische Ansätze zur Erklärung der Datenpreisgabe bei datenintensiven Anwendungen geworfen.

Zhou (2012) untersuchte die Nutzungsintention von ortsbasierten Diensten unter Einbezug von privatheitsrelevanten Faktoren. Ortsbasierte Dienste stellen eine Klasse von Diensten dar, die personalisierte, ortsbezogene Inhalte und Empfehlungen auf der Basis von der Position und den Präferenzen der Nutzenden anbieten. Auf der Basis der UTAUT konzipierte Zhou ein Modell, dass mit den klassischen UTAUT-Faktoren die begünstigenden Einflussfaktoren den hemmenden privatheitsbezogenen Faktoren für die Nutzungsintention von ortsbasierten Diensten gegenüberstellt (siehe Abbildung 10). Letztere umfassen *Privatheitsbedenken (engl. Privacy concerns),* das *Vertrauen in den Anbieter* (*engl. Trust in the provider*) und das *wahrgenommene Risiko* (engl. P*erceived risk*). Die *Privatheitsbedenken* beschreiben die Bedenken der Nutzenden bezüglich ihrer informationellen Privatheit (Xu et al., 2013), können jedoch als mehrdimensionales Konstrukt mit den Facetten Datenerfassung, Kontrolle und Bewusstsein aufgefasst werden (Malhotra et al., 2004a).

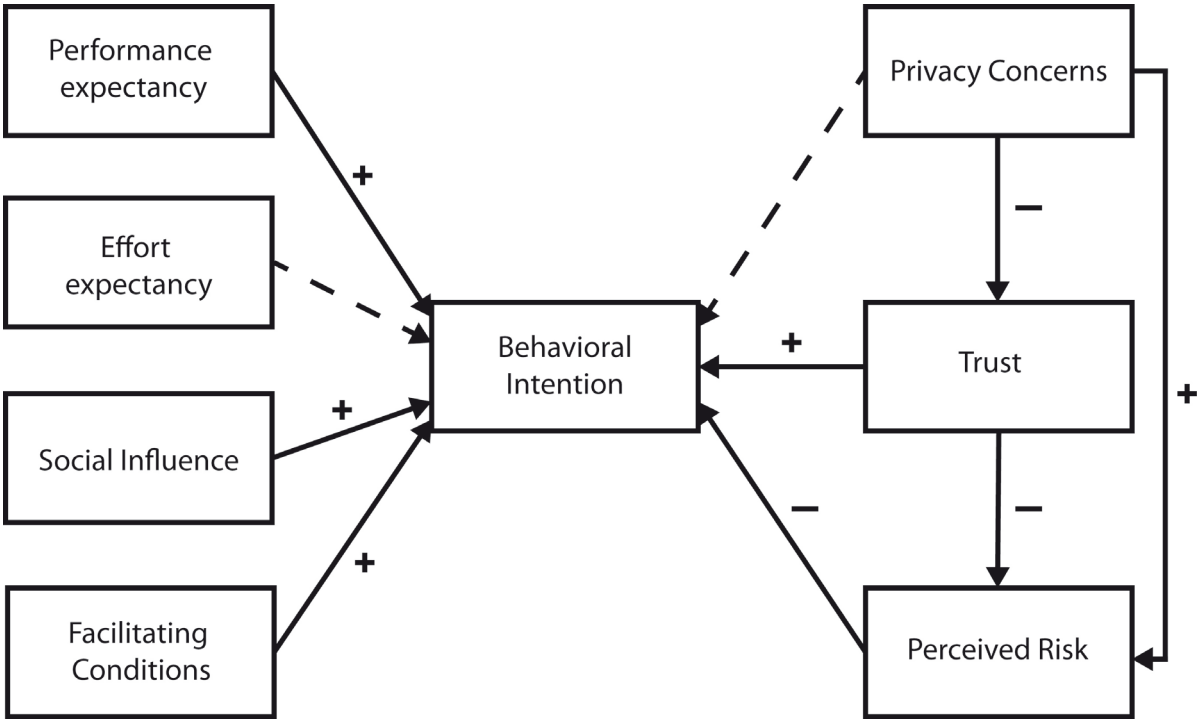


Abbildung 10. Modell zur Erklärung der Nutzungsintention von ortsbasierten Diensten nach Zhou (2012). Gestrichelte Linien stellen vorhergesagte, aber nicht empirisch bestätigte Beziehungen dar. „+" kennzeichnet einen positiven beziehungsweise verstärkenden Einfluss, „-" einen negativen beziehungsweise hemmenden Einfluss.

Das *Vertrauen in den Anbieter* hingegen kann als Bereitschaft der vertrauenden Person verstanden werden, sich auf der Basis einer positiven Erwartung bezüglich des zukünftigen Verhaltens des Interaktionspartners in eine Position der Verletzbarkeit zu begeben (Mayer et al., 1995). In Abgrenzung zu den *Privatheitsbedenken* beschreibt das *wahrgenommene Risiko* eine Gewichtung eines potentiellen Verlusts, der durch die Nutzung eines Systems eintreten könnte, mit der subjektiv wahrgenommenen Wahrscheinlichkeit des Eintretens dieses Verlusts (Cunningham, 1967). Im Kontext der Datenpreisgabe kann das *wahrgenommene Privatheitsrisiko* als die wahrgenommene Wahrscheinlichkeit des Kontrollverlusts über personenbeziehbaren Daten aufgefasst werden (Lee, 2009). Zhous Modell kann auch als eine Spezifizierung des privacy calculus Modells (Dinev & Hart, 2006; siehe Kapitel 2.2) verstanden werden, in dem auf der linken Seite die wahrgenommenen Vorteile und auf der rechten Seite des Modells die antizipierten Privatheitskosten aufgeführt sind.

Xu und Gupta (2009) untersuchten ebenfalls auf der Basis der UTAUT die Akzeptierbarkeit und Akzeptanz von ortsbasierten Diensten unter Einbeziehung von potentiellen Nutzenden (Akzeptierbarkeit) und erfahrenen Nutzenden (Akzeptanz). Die Autoren fanden, dass Privatheitsbedenken einen Einfluss auf die Leistungs- und Aufwandserwartung zur Vorhersage der Akzeptanz von ortsbasierten Diensten hat, während Privatheitsbedenken zur Vorhersage der Akzeptierbarkeit nur die Aufwandserwartungen negativ beeinflusste.

Xu et al. (2009) erweiterten das privacy calculus Modell um privatheitsbezogene Mechanismen wie monetäre Kompensationen für die Datenpreisgabe, industrielle Selbstregulationen sowie behördliche Regulationen zur Erklärung der Datenpreisgabe im Kontext von ortsbezogenen Diensten. Unabhängig von der anordnenden Institution hatten (Selbst-)Regulationen einen mindernden Effekt auf die wahrgenommenen Privatheitsrisiken. Monetäre Kompensationen erhöhten die wahrgenommenen Vorteile durch die Datenpreisgabe im Kontext von ortsbasierten Diensten nur dann, wenn die Dienste automatisch personalisierte Vorschläge und Informationen lieferten. Wurden diese von den Nutzern aktiv angefragt, hatten monetäre Kompensationen keinen Effekt auf die wahrgenommenen Vorteile.

Hsu und Lin (2016) adoptierten ebenfalls das privacy calculus Modell um die Nutzung von IoT-Diensten vorherzusagen. Die Autoren erweiterten das privacy calculus Modell um die Einstellung gegenüber der Nutzung von IoT-Services, ersetzten das wahrgenommene Privatheitsrisiko durch Privatheitsbedenken und modellierten die Privatheitsbedenken als ein mehrdimensionales Konstrukt, das sich in die Subfaktoren Datensammlung, unerlaubte Zweitverwendung von Daten, unangemessener Datenzugriff und fehlerhafte personenbeziehbare Daten aufgliedern lässt.

Auch Kowatsch und Maass (2012) testeten die Bereitschaft zur Datenpreisgabe im Kontext von IoT-Diensten mit Hilfe eines Modells, das die Autoren primär vom privacy calculus Modell ableiteten. Auf Basis der Evaluation von 31 IoT-Experten fanden die Autoren für den Anwendungsfall eines intelligenten Navigationsdienstes, dass die wahrgenommenen Privatheitsrisiken einen direkten Einfluss auf die Nutzungsintention des Navigationsdienstes haben. Weder Privatheitsbedenken noch das Vertrauen in den Anbieter des Navigationsdienstes mediierten diesen Einfluss. Im Gegensatz zu den vorherigen Studien basiert die Modellevaluation von Kowatsch und Maass auf einer sehr kleinen Stichprobe von Experten, deren Sichtweise und Bewertungsgrundlagen sich womöglich von denen durchschnittlicher Nutzenden unterscheidet.

Zusammengefasst zeigen diese Studien, dass Faktoren der Privatheit im IoT-Kontext eine bedeutende Rolle für die Bereitschaft, ein vernetztes System oder Dienst zu nutzen, spielen. Aufgrund der strukturellen Ähnlichkeiten zum IoT scheint eine Übertragbarkeit der Erkenntnisse auf das vernetzte Automobil möglich, steht jedoch noch aus. Obwohl mehrere Nutzendenbefragungen die Relevanz von Transparenz und Kontrolle über die Datenpreisgabe sowohl im vernetzten Automobil (siehe Kapitel 2.3.1) und im IoT-Kontext im Allgemeinen (Buck et al., 2017; Emami-Naeini et al., 2006) aufzeigen, hat die Informationskontrolle als potentiell relevanter Faktor für die Nutzungsintention eines vernetzten Systems noch keine Berücksichtigung in den obigen Modellen gefunden. Dabei konnten unter anderem Xu et al. (2013) für die Nutzung von

sozialen Medien nachweisen, dass die Kontrolle über die Datenpreisgabe nicht nur von Nutzenden in dezidierten Umfragen gefordert wird, sondern auch ein entscheidender Faktor für die Vorhersage zur Bereitschaft zur Datenpreisgabe im Zuge der Nutzung von datenintensiven Anwendungen sein kann.

2.7. Zusammenfassung und Ableitung der Forschungsfragen

Die Vernetzung des Automobils ermöglicht eine Vielzahl von neuen Funktionen im Fahrzeug, die die Sicherheit, die Effizienz als auch den Komfort des Automobils erhöhen. Wie Kapitel 2.3.1 zeigt, nehmen Nutzende diesen Mehrwert wahr, haben jedoch gleichzeitig Privatheitsbedenken, die durch die derzeitigen Datenschutzpraktiken nicht ausreichend bedient werden. Vielmehr fordern Nutzende ein Mehr an Transparenz und Kontrolle, wer wann wie die von ihnen preisgegebenen Daten verarbeitet. Gestützt werden sie dabei durch die juristischen Vorgaben der DSGVO, die mit ihren Schutzzielen unter anderem eine erhöhte Transparenz der Datenverarbeitung vorgibt. Während erste integrative Ansätze zur Ermöglichung einer selbstbestimmten Datenschutzkontrolle im vernetzten Automobil oder in verwandten IoT-Kontexten in der Forschungsgemeinde vorgeschlagen wurden, mangelt es noch an der theoretischen Abbildung der Relevanz von Privatheitsbedenken im Kontext des vernetzten Automobils. Wie die Kapitel 2.4 und 2.5 zeigen, werden verschiedene klassische Theorien zur Erklärung der Nutzung von technischen Systemen herangezogen, um auch die Akzeptierbarkeit und Akzeptanz von automobilen Anwendungen zu erklären. Entgegen der zahlreichen Befunden zur Relevanz der Privatheit in vernetzten Automobilen aus Nutzenden-, aber auch aus der juristischen und IT-Perspektive (siehe Kapitel 2.3), enthalten diese Modelle bislang keinen Privatheitsaspekt, der der wahrgenommenen Relevanz von Privatheit im vernetzten Automobil aus Nutzendensicht gerecht werden würde. Gleichzeitig zeigen aber Modellierungen aus anderen datenintensiven Nutzungskontexten, dass Privatheitsfaktoren eine bedeutende Rolle bei der Nutzungsentscheidung von Anwendungen spielen können (siehe Kapitel 2.6). Daher ist ein Ziel dieser Arbeit zu klären, ob die Wichtigkeit der informationellen Privatheit nicht nur in Befragungen von Nutzenden bekundet wird, sondern auch die Akzeptierbarkeit und Akzeptanz von vernetzten Diensten im Automobil entscheidend mitbeeinflusst:

Forschungsfrage 1:

Beeinflusst die Datenpreisgabe die Akzeptierbarkeit und Akzeptanz von vernetzten Diensten im Automobil?

Ebenso wie die DSGVO fordern auch Nutzende eine höhere Transparenz der Datenerfassung und –verarbeitung. Kapitel 2.3.1 zeigt, dass Nutzende noch einen Schritt weiter gehen und

neben der erhöhten Transparenz eine bessere Kontrolle über die preisgegebenen Daten einfordern. Eine Studie von Xu et al. (2013) im Kontext von sozialen Medien zeigt, dass die wahrgenommene Kontrollmöglichkeit über die preiszugebenen Daten die Absicht zur Preisgabe in der Tat beeinflusst. Dabei ist jedoch zwischen der *wahrgenommen* Informationskontrolle und der *tatsächlichen* Informationskontrolle zu unterscheiden, wie bereits in Kapitel 2.4.3 im Zuge der Einführung der Theory of Planned Behavior hingewiesen wurde. Gemäß den Konzepten der Theory of Planned Behavior umfasst die wahrgenommene Informationskontrolle auch Aspekte früherer Kontrollerfahrungen, ist aber nicht mit der tatsächlichen Kontrollerfahrung per se in der aktuellen Nutzungssituation gleichzusetzen. Vielmehr kann die wahrgenommene Kontrolle als Stellvertretung der tatsächlichen Kontrolle dienen (Ajzen, 1991). Die in Kapitel 2.3.2 vorgestellten integrativen Ansätze zur Wahrung der Privatheit im vernetzten Automobil bieten den Nutzenden die von ihnen eingeforderten Kontrolle über die Datenpreisgabe. Während die Theory of Planned Behavior eine Grundlage darstellt, um die Folgen einer tatsächlichen Kontrollerfahrung auf die Nutzungsintention zu antizipieren, existiert noch keine Untersuchung hierzu im Anwendungskontext des vernetzten Automobils. Daher lautet die zweite Forschungsfrage:

Forschungsfrage 2:

Verändert sich die Akzeptanz von vernetzten Diensten durch die Möglichkeit zur selbstbestimmten Datenpreisgabe im Vergleich zur Dienstnutzung ohne Kontrolle über die preiszugebenden Daten?

Um diese Forschungsfragen anzugehen, wird eine Simulatorstudie durchgeführt, mittels derer ein Modell zur Erklärung der Nutzungsintention von vernetzten Diensten im Automobil unter Berücksichtigung der Datenpreisgabe etabliert werden soll (Forschungsfrage 1). Die gleiche Studie umfasst einen Vergleich der Nutzungsintention eines vernetzten Dienstes vor und nach der Möglichkeit zur selbstbestimmten Datenschutzkontrolle (Forschungsfrage 2). Um die Aussagekraft des etablierten Modells zu erweitern, wird das Modell in zwei Replikationsstudien auf Basis der in Kapitel 2.1.1 vorgestellten Systematisierung von vernetzten Diensten im Automobil anhand von zwei weiteren Diensten getestet. Im folgenden Kapitel wird ein Modell zur Erklärung der Nutzungsintention von vernetzten Diensten im Automobil unter Berücksichtigung der Datenpreisgabe abgeleitet und die mit den Forschungsfragen 1 und 2 verbundenen Hypothesen aufgestellt.

3. Hypothesen und Untersuchungsmodell

Vernetzte Dienste im Automobil bieten eine Vielzahl verschiedener Vorteile, die jedoch mit der Preisgabe von (potentiell) personenbeziehbaren Daten einhergehen. Während zahlreiche Umfragen bereits aufgezeigt haben, dass Nutzende diesen Zwiespalt zwischen vermehrter Funktionalität und einem Eingriff in die informationelle Privatheit wahrnehmen, fehlt eine entsprechende Abbildung in der theoretischen Modellierung der Akzeptierbarkeit und Akzeptanz.

Wie Kapitel 2.5 zeigt stellen das TAM sowie die Theory of Planned Behavior auch im Automobil die dominanten klassischen Theorien dar. Daher basiert auch das hier vorgestellte Modell auf dem TAM, das unter anderem um Konstrukte der Theory of Planned Behavior ergänzt wird. Studien von Chen und Chen (2009) sowie Yoon und Cho (2016) zeigen, dass die wahrgenommene Nützlichkeit und die Einfachheit der Nutzung wichtige Determinanten für die Nutzungsintention von Systemen im Automobil sind. In Anlehnung an Davis (1989) wird die wahrgenommene Nützlichkeit hier als das Ausmaß definiert, in dem eine Person glaubt, dass die Nutzung eines vernetzten Dienstes im Automobil ihre Fahrt bereichert. Wie bereits Unterkapitel 2.4.3 zeigte, stellt die wahrgenommene Nützlichkeit eine der Determinanten der Einstellung gegenüber der Nutzung eines Systems sowie der Nutzungsintention dar (Chung et al., 2010; Müller-Seitz et al., 2009). Daher wird die wahrgenommene Nützlichkeit auch im Kontext von vernetzten Diensten im Automobil als wichtiger Faktor betrachtet, für den die folgenden Hypothesen formuliert werden können:

Hypothese 1.1: Die wahrgenommene Nützlichkeit hat einen signifikanten positiven Einfluss auf die Einstellung gegenüber der Nutzung von vernetzten Diensten im Automobil.

Hypothese 1.2: Die wahrgenommene Nützlichkeit hat einen signifikanten positiven Einfluss auf die Nutzungsintention von vernetzten Diensten im Automobil.

Ein weiterer grundlegender Faktor des TAM ist die Einfachheit der Nutzung eines Systems. In dem Kontext von vernetzten Automobilen kann die Einfachheit der Nutzung als das Ausmaß definiert werden, in dem Nutzende glauben, dass die Nutzung von vernetzten Diensten im Automobil aufwandsarm ist. Über mehrere Kontexte hinweg konnte gezeigt werden, dass eine einfache, aufwandsarme Nutzung sowohl die wahrgenommene Nützlichkeit erhöht als auch die Einstellung gegenüber der Nutzung des Systems positiv beeinflusst (Boer et al., 2019; Chen & Chen, 2009; Davis et al., 1989). Daher werden für die Nutzung vernetzter Dienste im Automobil folgende Hypothesen aufgestellt:

Hypothese 1.3: Die wahrgenommene Einfachheit der Nutzung beeinflusst die wahrgenommene Nützlichkeit positiv.

Hypothese 1.4: Die wahrgenommene Einfachheit der Nutzung beeinflusst die Einstellung gegenüber der Nutzung des Systems positiv.

Die Einstellung gegenüber der Nutzung eines Systems ist sowohl im TAM als auch in der Theory of Reasoned Action ein zentraler Prädiktor der Nutzungsintention. In Anlehnung an Davis (1986) kann sie hier als die affektive Bewertung der Nutzung eines vernetzten Dienstes im Automobil definiert werden. Da die zentrale Rolle der Einstellung gegenüber der Nutzung als direkte Antezedens der Nutzungsintention auch im Automobilkontext bereits mehrfach nachgewiesen werden konnte (Chen et al., 2007; Chen & Chen, 2009; Park et al., 2015), wird hier folgende Hypothese für die Nutzung vernetzter Dienste im Automobil aufgestellt:

Hypothese 1.5: Die Einstellung gegenüber der Nutzung des Systems hat einen positiven Effekt auf die Intention zur Nutzung von vernetzten Diensten im Automobil.

Die soziale Norm entstammt der Theory of Planned Behavior und kann im Kontext von vernetzten Diensten im Automobil als die normativen Überzeugungen einer Person, welche Erwartungen bedeutende Personen im nahen sozialen Umfeld mit Bezug auf die Nutzung solcher Dienste haben, verstanden werden. Sowohl für IT-Systeme im Allgemeinen (Gao & Bai, 2014; Lee, 2009; Leung & Chen, 2017) als auch im Automobil (Osswald et al., 2012) konnte der Einfluss des wahrgenommenen sozialen Drucks auf die Nutzungsintention nachgewiesen werden. Personen, die glauben durch die Nutzung von vernetzten Diensten im Automobil den Erwartungen ihres sozialen Umfelds zu entsprechen, sollten den vernetzten Dienst wahrscheinlicher nutzen, als solche, die diese normativen Überzeugungen nicht teilen. Daher wird hier postuliert:

Hypothese 1.6: Die soziale Norm hat einen positiven Einfluss auf die Intention zur Nutzung von vernetzten Diensten im Automobil.

Neben nutzen- und nutzungsbezogenen Einflussfaktoren auf die Nutzungsintention muss für vernetzte Dienste im Automobil auch der Umstand der Datenpreisgabe und somit der potentielle Eingriff in die informationelle Privatheit der Nutzenden abgebildet werden. Studien zu anderen datenintensiven Anwendungen wie IoT oder LBS können dabei als Referenz dienen, welche Privatheitsfaktoren bisher zur Abbildung der Privatheitsrelevanz Berücksichtigung fanden. Ebenso wie die in Kapitel 2.3.1 präsentierte Nutzendensicht auf das vernetzte Automobil heben auch diese Modelle die Privatheitsbedenken als einen entscheidenden Faktor zur Abbildung der Relevanz der Privatheit im vernetzten Automobil hervor. In Anlehnung an die oben genannte Definition von Xu et al. (2013) werden Privatheitsbedenken hier als die Bedenken eines Nutzenden über die Preisgabe von personenbeziehbaren Daten während der Interaktion mit einem vernetzten Dienst im Automobil definiert. Mehrere Studien haben bereits demonstriert, dass

Privatheitsbedenken dazu geeignet sind, um privatheitsbezogenen Verhaltensweisen vorherzusagen (Dinev & Hart, 2006; Li et al., 2019; Lowry et al., 2011; Malhotra et al., 2004a). Falls die informationelle Privatheit in der Tat an Relevanz im vernetzten Automobil gewinnt, sollten Privatheitsbedenken ein signifikanter Prädiktor der Nutzungsintention von vernetzten Diensten im Automobil sein. Nutzende von vernetzten Diensten könnten Bedenken bezüglich des Umgangs des Dienstanbieters mit den preisgegebenen Daten in Bezug auf die Datenerhebung, -speicherung und -nutzung hegen. Da Zhou (2012) für LBS zeigte, dass Privatheitsbedenken das wahrgenommene Privatheitsrisiko signifikant erhöhten, wird hier für vernetzte Dienste im Automobil angenommen:

Hypothese 1.7: Privatheitsbedenken haben einen positiven Einfluss auf das Privatheitsrisiko.

Darüber hinaus misstrauen Nutzende mit ausgeprägten Privatheitsbedenken besonders beim Umgang mit ihren Daten der Integrität von Dienstanbietern (Malhotra et al., 2004a; Zhou, 2012). Wie im Fall von anderen Kontexten wird erwartet, dass das Vertrauen in den Anbieter abnimmt, je höher die Privatheitsbedenken sind. Daher wird folgende Hypothese aufgestellt:

Hypothese 1.8: Privatheitsbedenken beeinflussen das Vertrauen in den Anbieter negativ.

Umfragen deuten wiederholt darauf hin, dass das Vertrauen in den Anbieter für Nutzende eine relevante Einflussgröße für die Nutzung von datenintensiven Diensten wie im vernetzten Automobil darstellt (siehe 2.3.1). Entsprechend hat das Vertrauen in den Anbieter auch eine prominente Rolle für die Vorhersage von Nutzungs- und Preisgabeverhalten in digitalen Kontexten, die von sozialen, informationellen oder materiellen Austausch geprägt sind, eingenommen (Dwyer et al., 2007; Gefen, Karahanna et al., 2003; Gefen, Rao et al., 2003; Wang & Lin, 2016). Dabei steigerte das Vertrauen in den Anbieter die Nutzungsintention, da es die Erwartung eines positiven zukünftigen Ergebnisses nährt (Zhou, 2012). Da auch die Datenpreisgabe im Kontext von vernetzten Diensten im Automobil als eine Form des Austausches betrachtet werden kann, wird hier angenommen:

Hypothese 1.9: Das Vertrauen in den Anbieter hat einen positiven Einfluss auf die Nutzungsintention von vernetzten Diensten im Automobil.

Unsicherheit ist eine Voraussetzung für die Notwendigkeit von Vertrauen. In Situationen, die als risikofrei beziehungsweise perfekt vorhersagbar wahrgenommen werden, gibt es keinen Grund sich auf das Vertrauen in eine Person oder Institution zu verlassen (Blau, 1964; Molm et al., 2000). Entsprechend konnten bisherige Studien eine enge Verbindung zwischen dem Vertrauen in einen Anbieter und dem wahrgenommenen Risiko in digitalen Umgebungen aufzeigen (Beldad et al., 2010; Pavlou, 2003; Zhou, 2012), bei der ein ausgeprägtes Vertrauen das

wahrgenommene Risiko reduziert (Gefen, Rao et al., 2003; Pavlou, 2003; Wang & Lin, 2016). Daher wird auch für den Kontext von vernetzten Diensten im Automobil angenommen:

Hypothese 1.10: Das Vertrauen in den Anbieter hat einen negativen Einfluss auf das wahrgenommene Privatheitsrisiko.

Wie bereits in Kapitel 2.6 eingeführt, kann das Privatheitsrisiko als die wahrgenommene (Un-) Sicherheit des Kontrollverlustes über personenbeziehbare Daten verstanden werden, das den potentiellen Missbrauch durch die datenerhaltende Partei mit einschließt (Lee, 2009). Im Kontext von vernetzten Diensten im Automobil sollte das wahrgenommene Privatheitsrisiko mit der Preisgabe von besonders kritischen Daten (wie zum Beispiel Gesundheitsdaten) oder der subjektiv hohen Wahrscheinlichkeit eines Datenmissbrauchs durch die datenempfangende Institution zunehmen. Verschiedene Studien haben bereits nachgewiesen, dass das wahrgenommene Privatheitsrisiko die Nutzungsintentionen direkt beeinflusst (Wang & Lin, 2016; Xu & Gupta, 2009). Sollten Nutzenden einen möglichen Kontrollverlust über die preiszugebenden Daten als wahrscheinlich bewerten, sind sie eher zurückhaltend gegenüber der Nutzung eines entsprechenden Produkts (Featherman et al., 2010). Darüber hinaus zeigt unter anderem Lee (2009), dass das wahrgenommene Privatheitsrisiko die affektive Bewertung der Nutzung eines Systems negativ beeinflusst. Daher werden folgende Hypothesen für vernetzte Dienste im Automobil aufgestellt:

Hypothese 1.11: Das wahrgenommene Privatheitsrisiko beeinflusst die Nutzungsintention von vernetzten Diensten im Automobil negativ.

Hypothese 1.12: Das wahrgenommene Privatheitsrisiko beeinflusst die Einstellung gegenüber der Nutzung von vernetzten Diensten im Automobil negativ.

In den vorangegangenen Kapiteln, die die Definition, Regelung und Wahrnehmung von Privatheit zum Inhalt hatten, spielte Kontrolle eine zentrale Rolle. Sowohl im Auge der Nutzenden (siehe Kapitel 2.3.1), in zentralen Definitionsansätzen von Privatheit (zum Beispiel Westin (1967); siehe auch Kapitel 2.2) und in regulatorischen Vorgaben (siehe Kapitel 2.3) konnte die Kontrolle über die preiszugebenden Daten als ein zentraler Faktor im Kontext von vernetzten Diensten im Automobil identifiziert werden. Die wahrgenommene Kontrolle spielt dabei auch in modell-theoretischen Ansätzen wie der Theory of Planned Behavior (Ajzen, 1985) eine entscheidende Rolle. Auch im Kontext von digitalen Systemen beschrieben Studien die Informationskontrolle als einen zentralen Prädiktor von Datenpreisgabe und Nutzungsintention. Dabei kann die Informationskontrolle als die wahrgenommenen internen und externen Möglichkeiten, die eine Person hat um preisgegebene Informationen zu kontrollieren, verstanden werden

(Xu et al., 2013). Wurde die Informationskontrolle als hoch wahrgenommen, sanken die Privatheitsbedenken als auch das wahrgenommene Privatheitsrisiko (Hajli & Lin, 2016; Xu et al., 2011; Xu et al., 2013). Daher wird für vernetzte Dienste im Automobil angenommen:

Hypothese 1.13: Die wahrgenommene Informationskontrolle beeinflusst das wahrgenommene Privatheitsrisiko negativ.

Hypothese 1.14: Das wahrgenommene Informationskontrolle beeinflusst die Privatheitsbedenken negativ.

Die aufgestellten Hypothesen ergeben das in Abbildung 10 zusammengefasste Akzeptanzmodell für vernetzte Dienste im Automobil, das in dieser Arbeit postuliert wird.

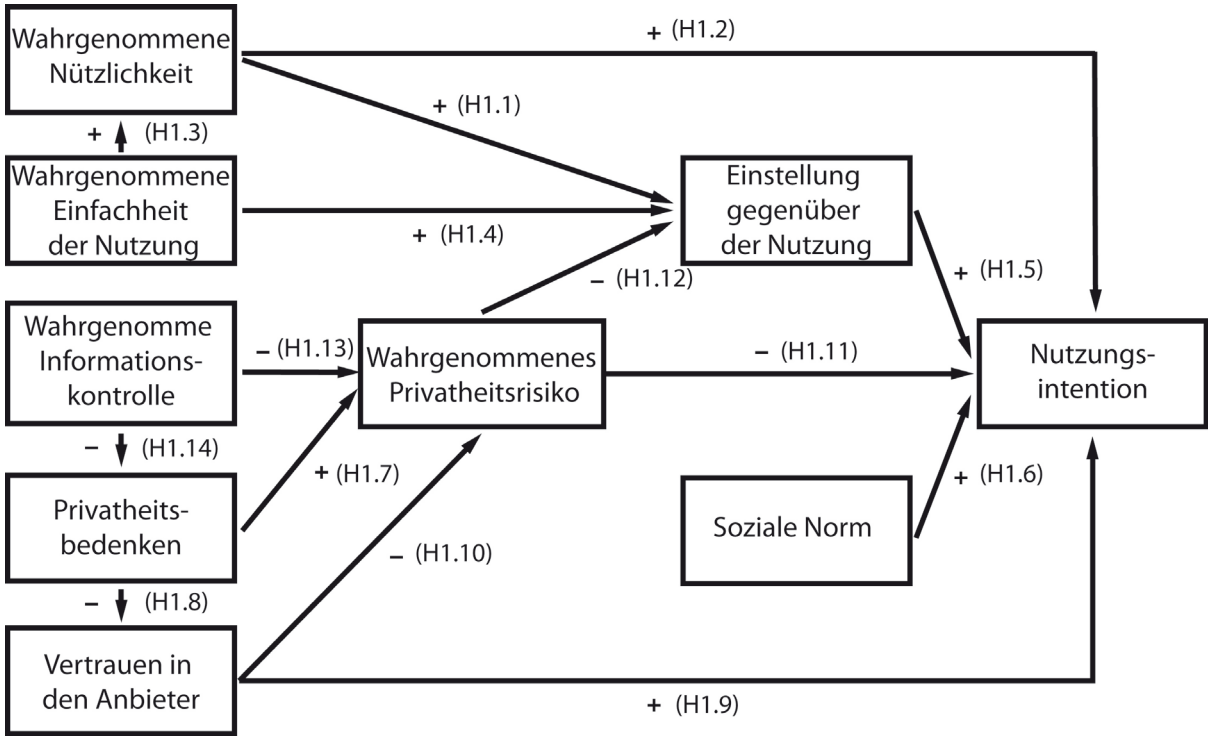


Abbildung 10. Hypothetisiertes Modell zur Erklärung der Akzeptierbarkeit und Akzeptanz von vernetzten Diensten im Automobil. „+" zeigt einen positiven, „-" einen negativen Einfluss an.

Während das obige Modell die wahrgenommene Kontrolle abbildet, wünschen sich Nutzende eine tatsächliche Kontrolle über die Datenpreisgabe (siehe Kapitel 2.3.1). Erste integrative Ansätze schlagen zwar bereits unterschiedliche Lösungen zur Ermöglichung einer nutzerzentrierten Kontrolle über die Datenpreisgabe vor (siehe Kapitel 2.3.2). Gleichzeitig existieren jedoch nur wenige Studien, die den Einfluss der tatsächlichen Informationskontrolle auf weitere privatheitsrelevante Faktoren durch experimentelle Variationen untersuchten (Gómez-Barroso, 2018). In Anlehnung an die Theory of Planned Behavior (Ajzen, 1985) zeigten Wilson et al.

(2015), dass tatsächliche Kontrollmöglichkeiten über die Datenpreisgabe nicht nur die wahrgenommene Informationskontrolle, sondern auch die Privatheitsbedenken beeinflussen. Arcand et al. (2007) untersuchten darüber hinaus die unterschiedlichen Einflüsse von Informationen über die Datenpreisgabe im Gegensatz zu tatsächlicher Informationskontrolle. Die Autoren konnten zeigen, dass die bloße Präsenz von Datenschutzerklärungen einen Einfluss auf die wahrgenommene Privatheitskontrolle hat, ohne dass sie eine tatsächliche Kontrolle bieten würde. Setzen sich Nutzende jedoch mit den Datenschutzerklärungen näher auseinander, haben nur solche Erklärungen einen positiven Effekt auf die wahrgenommene Privatheitskontrolle und das Vertrauen in den Anbieter, die als Default keine Datenpreisgabe erlauben (opt-in) und somit eine explizite Zustimmung zur Datenpreisgabe erfordern (Arcand et al., 2007).

Zwar gibt es im vernetzten Automobil noch keine systemübergreifenden Standards, wie Einwilligungen zur Datenpreisgabe kommuniziert und eingeholt werden. Allerdings besteht mit Android Auto ein *integrated system* Ansatz (siehe Kapitel 2.1), der auf der Spiegelung der Smartphoneinhalte auf die visuelle Schnittstelle des vernetzten Automobils basiert. Android bietet den Nutzenden beim Download einer neuen Applikation eine kompakte Übersicht über die preiszugebenden Daten, die jedoch einen rein informativen Charakter haben. Die Ergebnisse von Arcand et al. (2007) legen nahe, dass im vernetzten Automobil ein solcher Informationsbildschirm zwar bereits ein gehobenes Niveau der *wahrgenommenen* Informationskontrolle erzeugt. Haben Nutzende jedoch einen Zugriff auf Privatheitseinstellungen, die ihnen *tatsächliche* Kontrollmöglichkeiten im Sinne einer selbstbestimmten informationellen Privatheit aufzeigen, sollten unter letzterer Bedingung die wahrgenommene Informationskontrolle als auch das Vertrauen in den Anbieter höher sein als unter rein informierenden Anzeigen der preiszugebenden Daten. Daher wird für vernetzte Dienste im Automobil angenommen:

Hypothese 2.1: Die Erfahrung einer tatsächlichen Kontrolle über die Preisgabe von Daten während der Nutzung von vernetzten Diensten im Automobil führt zu einer höheren wahrgenommenen Informationskontrolle als unter der Präsenz eines privatheitsbezogenen Informationsbildschirms.

Hypothese 2.2: Die Erfahrung einer tatsächlichen Kontrolle über die Preisgabe von Daten während der Nutzung von vernetzten Diensten im Automobil führt zu einem höheren Vertrauen in den Anbieter als unter der Präsenz eines privatheitsbezogenen Informationsbildschirms.

Die Ergebnisse von Wilson et al. (2015) legen nahe, dass auch im vernetzten Automobil das Vorliegen einer tatsächlichen Kontrolle über die Datenpreisgabe nicht nur zur Erhöhung der wahrgenommenen Privatheitskontrolle, sondern auch zu einer Reduzierung der Privatheitsbedenken führt. Daher wird folgende Hypothese für vernetzte Dienste im Automobil aufgestellt:

Hypothese 2.3: Die Erfahrung einer tatsächlichen Kontrolle über die Preisgabe von Daten während der Nutzung von vernetzten Diensten im Automobil führt zu geringeren Privatheitsbedenken als unter der Präsenz eines privatheitsbezogenen Informationsbildschirms.

Führt die Erfahrung einer tatsächlichen Kontrolle über die Datenpreisgabe zu einer Erhöhung der wahrgenommenen Informationskontrolle, so sagen die Studienergebnisse von Hajli und Lin (2016) voraus, dass sich solche Effekte indirekt auch auf das wahrgenommene Privatheitsrisiko auswirken. Daher wird für vernetzte Dienste im Automobil angenommen:

Hypothese 2.4: Die Erfahrung einer tatsächlichen Kontrolle über die Preisgabe von Daten während der Nutzung von vernetzten Diensten im Automobil führt zu einem geringeren wahrgenommenen Privatheitsrisiko als unter der Präsenz eines privatheitsbezogenen Informationsbildschirms.

In dem in Abbildung 10 präsentierten Modell zur Erklärung der Akzeptierbarkeit und Akzeptanz von vernetzten Diensten im Automobil wird die Einstellung gegenüber der Nutzung eines solchen Dienstes sowohl von privatheitsbezogenen als auch von nutzungsbezogenen Faktoren beeinflusst. Wilson et al. (2015) konnten jedoch zeigen, dass die Möglichkeit zur Kontrolle über die Datenpreisgabe auch die Einstellung positiv beeinflusst. Daher wird auch für den Kontext des vernetzten Automobils folgende Hypothese aufgestellt:

Hypothese 2.5: Die Einstellung gegenüber der Nutzung von vernetzten Diensten im Automobil ist unter dem Vorhandensein einer tatsächlichen Kontrollmöglichkeit über die Preisgabe von Daten positiver als unter der Präsenz eines privatheitsbezogenen Informationsbildschirms.

In Akzeptanzmodellen dient die Nutzungsintention klassischerweise als Stellvertretung für die Akzeptierbarkeit oder Akzeptanz. Eine besondere Bedeutung würde dem Vorliegen einer tatsächlichen Kontrollmöglichkeit zukommen, wenn diese nicht nur einzelne privatheitsbezogene Bewertungen, Überzeugungen und Einstellungen beeinflusst, sondern darüber hinaus auch handlungsleitend ist. In der Tat legen bisherige Studien nahe, dass die Möglichkeit zu einer tatsächlichen Kontrolle über die Datenpreisgabe zu einer höheren Nutzungsintention führt. Gideon et al. (2006) und Tsai et al. (2011) manipulierten jeweils die Verfügbarkeit und Zugänglichkeit von Datenschutzerklärungen beim Online-Shopping und fanden heraus, dass das Einkaufsverhalten sowie die Bereitschaft zur Datenpreisgabe währenddessen durch die experimentellen Manipulationen positiv beeinflusst wurden. Tucker (2014) variierte die Kontrolle über die preiszugebenden Informationen im Kontext der Nutzung von personalisierter Werbung. Ein Mehr an Informationskontrolle verleitete Nutzende dazu, personalisierter Werbung doppelt so häufig zuzustimmen als unter der Bedingung einer niedrigen Informationskontrolle.

Auch Lee et al. (2011) zeigten, dass explizite Kontrollmechanismen das Bewusstsein für den Schutz der informationellen Privatheit erhöhen, sodass die Intention zur Datenpreisgabe erhöht wird. Daher wird auch für den Kontext von vernetzten Diensten im Automobil angenommen:

Hypothese 2.6: Die Nutzungsintention von vernetzten Diensten im Automobil ist unter dem Vorhandensein einer tatsächlichen Kontrollmöglichkeit über die Preisgabe von Daten höher als unter der Präsenz eines privatheitsbezogenen Informationsbildschirms.

Die Hypothesen zu Forschungsfrage 2 sind in Abbildung 11 zusammengefasst.

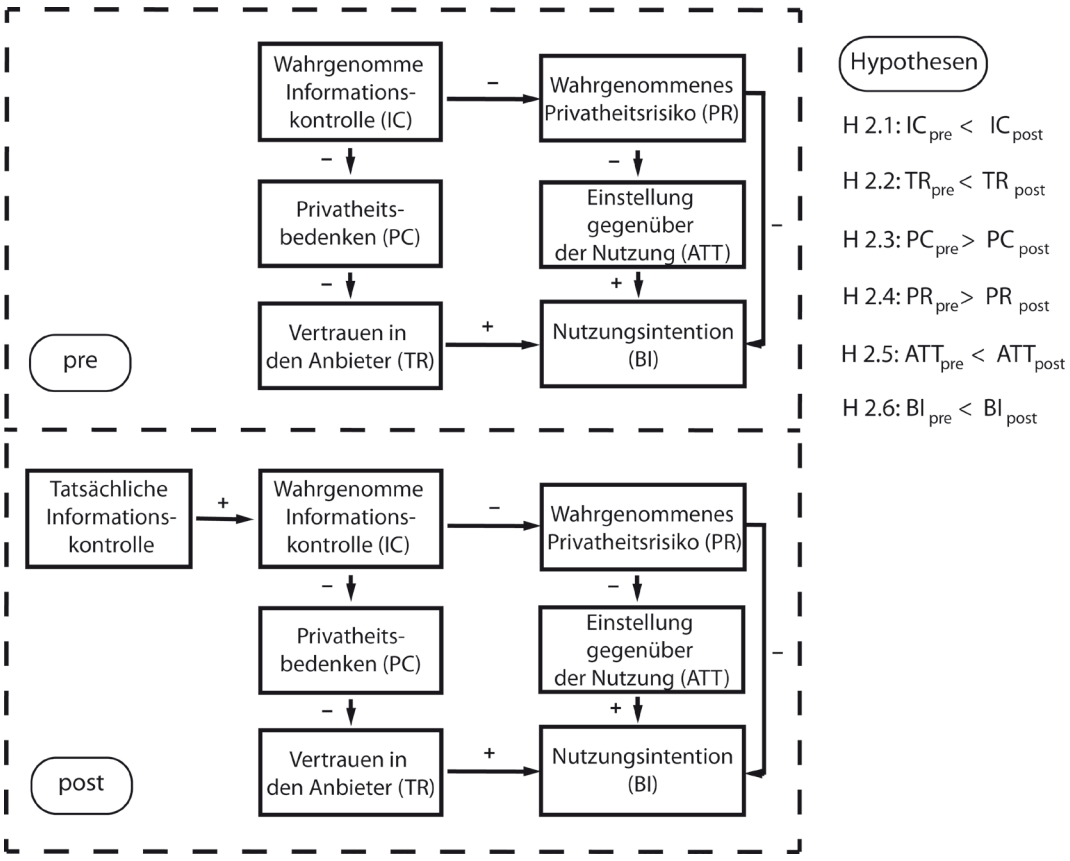


Abbildung 11. Darstellung des erwarteten Einflusses der tatsächlichen Informationskontrolle auf die betrachteten privatheitsbezogenen Faktoren. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

4. Empirische Untersuchung

Zur Untersuchung der beiden Forschungsfragen werden drei Studien durchgeführt. Während alle drei Studien zur Beantwortung der Forschungsfrage 1 beitragen, wird im Zuge der ersten Studie im Fahrsimulator die dafür notwendige Methodik etabliert. Gleichzeitig dient Studie 1 zur Beantwortung der Forschungsfrage 2. Daher stellt Studie 1 die Hauptuntersuchung dar, während die Studien 2 und 3 Replikationsstudien sind, die auf der Basis von Online-Befragungen zur Untersuchung der Tragweite des in Studie 1 etablierten Modells dienen.

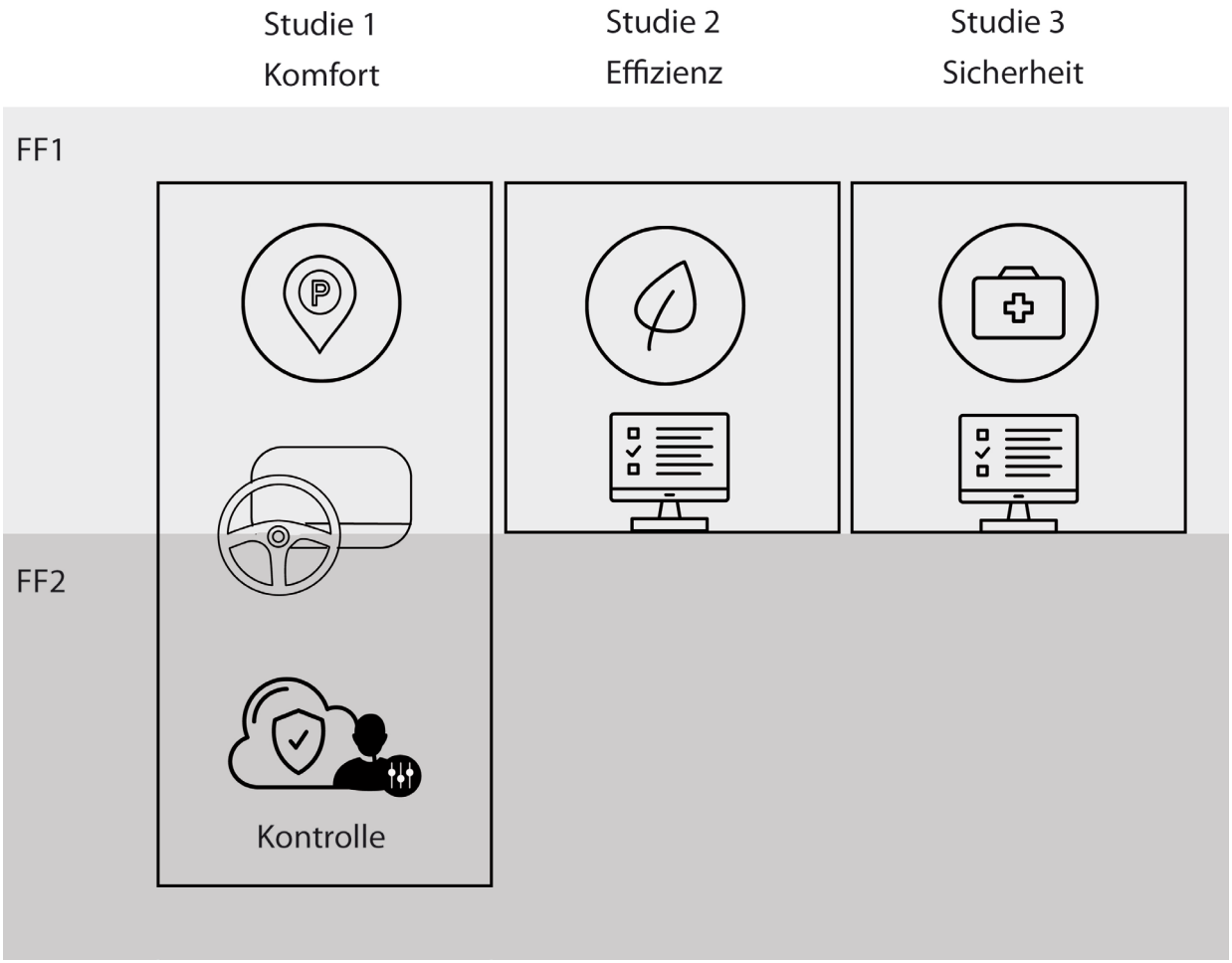


Abbildung 12. Zusammenfassung des Vorgehens zur Beantwortung der Forschungsfragen (FF) 1 und 2. Während FF 1 durch die Studien 1-3 behandelt wird, wird FF 2 im Zuge von Studie 1 untersucht. Studie 1 stellt die Hauptstudie dar und findet im Fahrsimulator statt, während die Studien 2 und 3 Replikationsstudien darstellen, die mittels eines Online-Fragebogens durchgeführt werden. In Studie 1 kommt ein komfortbezogener vernetzter Mehrwertdienst zum Einsatz, während die Replikationsstudien jeweils einen effizienzbezogenen (Studie 2) beziehungsweise einen sicherheitsbezogenen vernetzten Mehrwertdienst (Studie 3) beinhalten.

Nach Walter et al. (2020) können vernetzte Mehrwertdienste im Automobil in die funktionalen Kategorien *Komfort, Effizienz* und *Sicherheit* gegliedert werden. Daher kommen in den Studien 1 bis 3 ein komfortbezogener (Studie 1), ein effizienzbezogener (Studie 2) und ein sicherheitsbezogener vernetzter Mehrwertdienst (Studie 3) zum Einsatz. Abbildung 12 fasst das Vorgehen zusammen.

4.1. Studie 1: Etablierung des Modells und Untersuchung des Einflusses einer tatsächlichen Kontrolle über die Datenpreisgabe

Einer der Hauptgründe für die Verkehrsmittelwahl zu Gunsten des privaten Automobils ist die Privatheit, die das Automobil unter anderem beim Pendeln verspricht (Gardner & Abraham, 2007). Durch die Vernetzung des Automobils wird ein Datenfluss in und aus dem Automobil heraus etabliert, der eine potentielle Einschränkung der informationellen Privatheit der Nutzenden darstellen kann (Hansen, 2015). Daher gewinnt die informationelle Privatheit mit Einführung von vernetzten Diensten im Automobil an Relevanz, die zwar von Nutzenden, der Regulatorik und IT-Sicherheitsexperten artikuliert wird (siehe Kapitel 2.3), jedoch noch keinen Einzug in die Akzeptanzmodellierung im Kontext des Fahrzeugs gehalten hat. Die erste Studie zielt entsprechend auf die Etablierung eines Modells zur Erklärung der Nutzungsintention von vernetzten Diensten im Automobil unter Berücksichtigung der Datenpreisgabe ab (Forschungsfrage 1; Hypothesen H 1.1 bis H 1.14) und untersucht darüber hinaus den Einfluss der Möglichkeit zur tatsächlichen Informationskontrolle auf die Akzeptanz von vernetzten Diensten im Automobil (Forschungsfrage 2; Hypothesen H 2.1 bis H 2.6). Die Studie wurde im Fahrsimulator des Instituts für Arbeitswissenschaft der Technischen Universität Darmstadt mit der Unterstützung bei der Datenerhebung von Charlotte Ebeling, Marie Bode, Johanna Vetter, Eugen Sommer, Robin Schmitt und Marco Klumpp im Zuge von studentischen Arbeiten durchgeführt (Bode, 2018; Ebeling, 2018; Klumpp & Schmitt, 2018; Sommer, 2018; Vetter, 2018).

4.1.1. Methodik

Teilnehmende. 116 Teilnehmende wurden in Studie 1 eingeschlossen (50 Frauen, 66 Männer; M_{Alter} = 30,47 Jahre, SD_{Alter}= 12,43 Jahre). Alle Teilnehmenden berichteten eine normale oder korrigierte Sehfähigkeit zu haben, waren im Besitz eines gültigen Führerscheins (mindestens) der Klasse B und besaßen ein Smartphone, welches sie mit zur Studiendurchführung bringen mussten. Neben dem Alter und dem Geschlecht wurden auch die durchschnittliche Smartphonenutzung sowie der Kenntnisstand bezüglich vernetzter Automobile vor der Teilnahme an der Studie abgefragt. Nur 2 von 116 Teilnehmenden (1,72 %) berichteten ihr Smartphone nicht täglich zu benutzen. 83 von 116 Teilnehmenden (71,55 %) gaben an bereits vor der Studienteilnahme von vernetzten Automobilen gehört zu haben.

Tabelle 4. Zusammenfassung der Informationen über die Stichprobe.

Alter		Geschlecht		Kenntnis vor Studie		Smartphonenutzung	
M	30,47 J.	M	66	Ja	83	Täglich	114
SD	12,42 J.	W	50	Nein	33	Unregelmäßig	2

Die Informationen zu den Teilnehmenden der Studie sind in Tabelle 4 zusammengefasst. Die Teilnehmenden wurden im Umfeld der Technischen Universität Darmstadt sowie im privaten Umfeld des Autors rekrutiert und erhielten eine Aufwandsentschädigung über 20 Euro für ihre Teilnahme. Das experimentelle Vorgehen orientierte sich strikt an den ethischen Richtlinien und Empfehlungen des Ethikkomitees der Technischen Universität Darmstadt. Entsprechend wurde von allen Teilnehmenden eine schriftliche Einverständniserklärung bezüglich der Teilnahme an der Studie eingeholt.

Fragebogenentwicklung. Zur Testung des aufgestellten Akzeptierbarkeits- und Akzeptanzmodells für vernetzte Dienste im Automobil wurde ein Online-Fragebogen gestaltet. Die darin enthaltenen Skalen wurden aus der existierenden Literatur abgeleitet und an den Kontext des vernetzten Automobils angepasst. Dabei wurden besonders solche Studien berücksichtigt, die entweder selbst im Kontext des Automobils beheimatet sind oder anderen datenintensiven Kontexten entstammen. Die Skalen für die wahrgenommene Nützlichkeit, die wahrgenommene Einfachheit der Nutzung, die Einstellung gegenüber der Nutzung eines Systems sowie die Intention zur Nutzung eines Systems wurden aus bestehenden Studien entnommen, die ebenfalls auf das TAM aufbauen (Chen & Chen, 2009; Davis, 1989; Ussat, 2012). Die Skalen für Privatheitsbedenken, das wahrgenommene Privatheitsrisiko und das Vertrauen in den Anbieter sind an Zhou (2012) angelehnt, während die Skala für die wahrgenommene Informationskontrolle Xu et al. (2013) entstammt. Die Items für die soziale Norm wurden Osswald et al. (2012) entnommen. Jede Skala verfügte über mindestens drei Items. Alle Items über alle Skalen hinweg wurden auf einer fünfstufigen Likert-Skala mit verbalen Ankern von *trifft absolut nicht zu* bis *trifft absolut zu* bewertet. Während dies für fast alle Skalen nur eine Übersetzung aus dem Englischen in das Deutsche bedeutete, wurde für die Skala zur wahrgenommenen Informationskontrolle zudem die Antwortskala von sieben Stufen auf fünf Stufen reduziert. Aufgrund der notwendigen Anpassungen durchlief der gesamte Fragebogen entsprechend den Empfehlungen von Hair et al. (2016) einen zweistufigen Pretest um die Validität und Reliabilität des Fragebogens zu gewährleisten. Zuerst wurden alle Skalen durch wissenschaftliche Mitarbeiter des Instituts für Arbeits-

wissenschaft in Hinblick auf die Inhaltsvalidität überprüft. Hierzu wurden Definitionen der Konstrukte bereitgestellt, sodass die inhaltliche Eignung der Items überprüft werden konnte. Anschließend wurde ein Pretest (N = 33) mit Teilnehmenden aus dem Bekanntenkreis des Autors durchgeführt. Das zweistufige Verfahren führte zu einer Umformulierung von Items der Skalen zur wahrgenommenen Nützlichkeit, dem wahrgenommenen Privatheitsrisiko sowie der Einstellung gegenüber der Nutzung des Systems. Tabelle A1 im Anhang bietet einen Überblick über die interne Konsistenz (Cronbach's α) der einzelnen Skalen im Pretest. Tabelle A2 stellt die finalen, in Studie 1 verwendeten Skalen dar. Für alle Skalen, die aufgrund der Ergebnisse des Pretests eine Änderung bedurften, wurden zusätzliche Items mitaufgenommen. Für die wahrgenommene Nützlichkeit lagen nach der Reformulierung und Generierung neuer Items sechs Items vor, von denen vier Items in Studie 1 in die Skalenberechnung einflossen. Für das wahrgenommene Privatheitsrisiko lagen vier Items vor, von denen drei in Studie 1 in die Skalenberechnung einflossen. Die Einstellung gegenüber der Nutzung des vernetzten Dienstes konnte mit vier Items abgebildet werden, von denen drei für die entsprechende Skala in Studie 1 verwendet wurden. Die Itemauswahl für die jeweiligen Skalen für Studie 1 wurde so getroffen, dass jeweils mindestens drei Items enthalten waren sowie die bestmöglichen Skaleneigenschaften mit Bezug auf die Gütekriterien erzielt werden konnten. Neben diesen Skalen wurden demographische Variablen (Alter, Geschlecht, Führerscheinbesitz, Häufigkeit der Nutzung eines Automobils sowie eines Smartphones), der Kenntnisstand bezüglich vernetzter Fahrzeuge vor der Versuchsteilnahme, das Vertrauen in verschiedene datenempfangende Parteien (Fahrzeughersteller, ConnCar AG, Polizei, Rettungsdienst, Versicherer, App-Anbieter und Verkehrsleitzentrale) sowie die wahrgenommene Sensibilität der preiszugebenden Daten (siehe Tabelle 5, erste Spalte) erhoben. Die Fragen zur wahrgenommenen Sensitivität der im Video preisgegebenen Daten wurden auf einer fünfstufigen Skala mit den Endpunkten *nicht persönlich* und *persönlich* beantwortet, während Items zum Vertrauen in unterschiedliche Entitäten eine fünfstufige Skala mit den Endpunkten *stimme gar nicht zu* und *stimme voll zu* bezogen auf die Aussage „Ich vertraue [...] im Umgang mit meinen Daten." benutzten.

Materialien und Apparaturen. Die Studie wurde in dem statischen Fahrsimulator des Instituts für Arbeitswissenschaft der Technischen Universität Darmstadt durchgeführt. Der Fahrsimulator ist mit einem Sichtfeld von 180° ausgestattet, das mit Hilfe von drei hochauflösenden Projektoren (Auflösung: 1920 x 1200 Pixel; Helligkeit: 6000 Lumen) erreicht wird. Der Fahrsimulator besteht aus einer Karosserie eines Chevrolet Aveo. Ein zehn Zoll großes Tablet (Auflösung: 1920 x 1200 Pixel) ist an der Mittelkonsole des Aveos als zentrales Touch-Display angebracht. Abbildung 13 zeigt den schematischen Versuchsaufbau inklusive des Fahrsimulators.

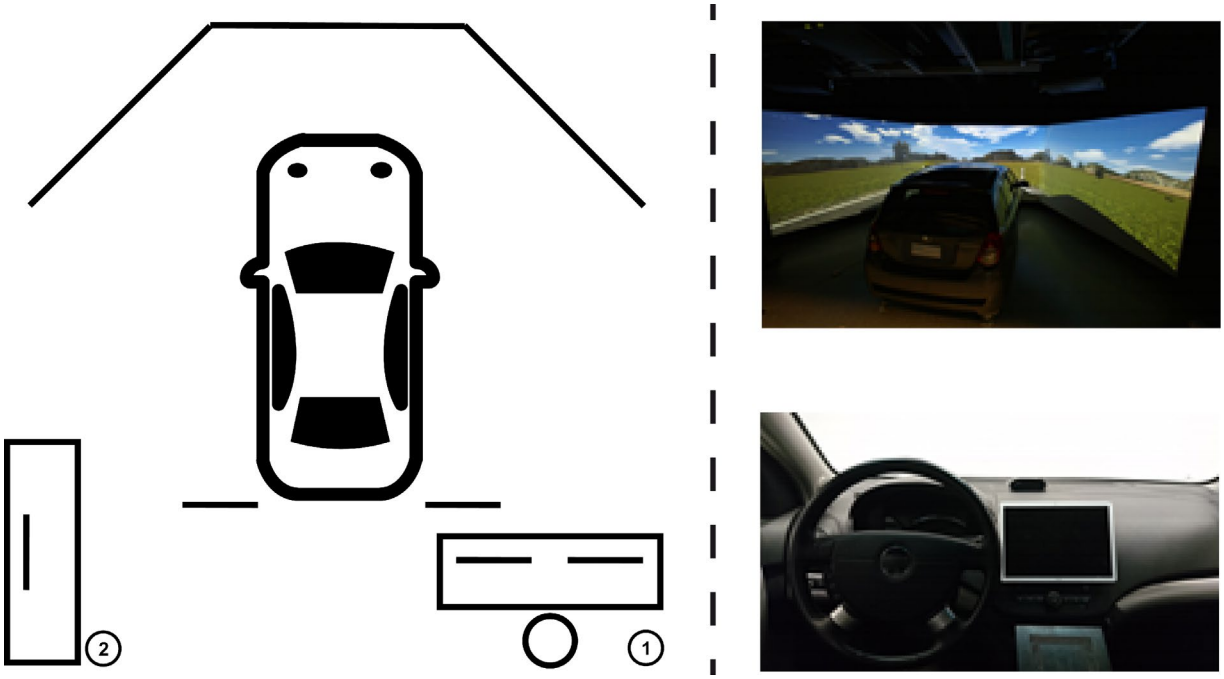


Abbildung 13. Versuchsaufbaus inklusive des statischen Fahrsimulators. *Links:* Schematische Darstellung. 1: Arbeitsplatz des Versuchsleitenden. 2: Computer zur Durchführung des Online-Fragebogens. *Rechts oben:* Blick auf Fahrsimulator. *Rechts unten:* Versuchsaufbau im Cockpit des MockUps.

Für die Studie wurde ein virtuelles Abbild eines Teils von Mannheim in SILAB erstellt (Dao, 2017). Das konkrete Streckenvorbild für die experimentelle Bedingung war die Route von L5 1 zum Café Vienna in S1. Das Egofahrzeug begegnete dabei mäßigem Verkehr, ohne dass es zu Beeinträchtigungen oder Blockaden der intendierten Fahrtrichtung kam. Jede Kreuzung und Abbiegung war mittels Ampeln geregelt, die bei der Annäherung des Egofahrzeugs auf Rot geschaltet wurden. Dies ermöglichte eine Wizard-of-Oz-Simulation, auf die im weiteren Verlauf dieses Unterkapitels näher eingegangen wird. Die Simulationsumgebung ging über die oben beschriebene Route hinaus, wobei solche Teile der Simulationsumgebung, die sich nicht auf dieser Route befanden, zur Trainingsfahrt im Sinne einer Eingewöhnung an die Simulationsumgebung genutzt wurde.

Der vernetzte Mehrwertdienst. Der komfort-bezogene vernetzte Mehrwertdienst für diese Studie stellt einen vernetzten Parkdienst dar und ist dem Konzept von He et al. (2014) nachempfunden. Der Parkdienst *Parking-App* verfügt über eine Navigationsfunktion, die um eine intelligente Parkplatzsuche und -reservierung erweitert ist. Jedes vernetzte Automobil agiert dabei unter Rückgriff auf die fahrzeugeigenen Umgebungssensoren als ein fahrender Sensor, der freie Parkplätze sowie deren zwischenzeitliche Belegung detektiert und der Allgemeinheit zur Verfügung stellt.

Ein interaktiver Click-Dummy des Parkdienstes wurde mit Hilfe des Wireframing-Programms AXURE RP 8 in Anlehnung an den menschzentrierten Produktentwicklungsprozess (ISO, 2011) erstellt (Wardak, 2017) und wurde anschließend durch den Autor weiter für das hiesige Studiendesign optimiert. Der Parkdienst liegt in vier verschiedenen Ausführungen vor (V1 bis V4), um das experimentelle Vorgehen dieser Studie zu ermöglichen (siehe dazu *Versuchsdurchführung* im weitere Verlauf dieses Unterkapitels). Die Ausführungen unterscheiden sich im Umfang der Datenpreisgabe sowie der verfügbaren Funktionen (siehe Tabelle 5). Die Default-Version des Parkdienstes bietet den vollen Funktionsumfang, erfordert jedoch die Preisgabe der Identität, der Kalendereinträge, des Fahrverhaltens, Daten von Umgebungssensoren des Automobils, des Standorts sowie der Zeit.

Tabelle 5. Varianten des vernetzten Parkdienstes mit Auflistung der jeweils preisgegebenen Daten sowie der verfügbaren Funktionen.

Variante	V1 (Default)	V2	V3	V4
PRICON Level	Niedrig	Mittel	Hoch	Maximal
Daten				
Standort	✓	✓	✓	✓
Fahrverhalten	✓	✓	✓	
Uhrzeit	✓	✓	✓	
Identität	✓	✓		
Kalendereinträge	✓			
Funktionen				
Navigation	✓	✓	✓	✓
Parkplatzortung	✓	✓	✓	
Manuelle Reservierung	✓	✓		
Terminbasierte Reservierung	✓			

Durch die Verbindung mit dem Smartphone des Nutzenden umfasst der volle Funktionsumfang des Parkdienstes eine terminbasierte Ortung und Reservierung eines Parkplatzes an dem im Kalendertermin eingetragenen Zielort sowie eine Navigation des Nutzenden zu dem reservierten Parkplatz. Der Parkdienst erhält durch die Kopplung mit dem Smartphone Zugriff auf die Kalendereinträge des Nutzenden, sodass die terminbasierte Parkplatzortung und –reservierung automatisch erfolgen kann (siehe Abbildung 14). Wie Tabelle 5 aufzeigt verhält sich der Funktionsumfang kongruent zur Datenpreisgabe: Je weniger Daten preisgegeben werden, desto weniger Funktionen stehen zur Verfügung. Die Navigationsfunktion wird durch eine Integration durch Screenshots von Mannheim in Google Maps (klassische Kartenansicht) sowie einer mit der erlaubten Geschwindigkeit auf der Route von Route von L5 1 zum Café Vienna in S1 abgestimmten Animation realisiert.

Das Interface zur Informationskontrolle. Das Datenschutzinterface PRICON des Projektes SeDaFa (Plappert et al., 2017; Walter et al., 2018) wurde in dieser Studie als Kontrollmöglichkeit über die Datenpreisgabe im Kontext der Nutzung von vernetzten Diensten im Automobil eingesetzt.

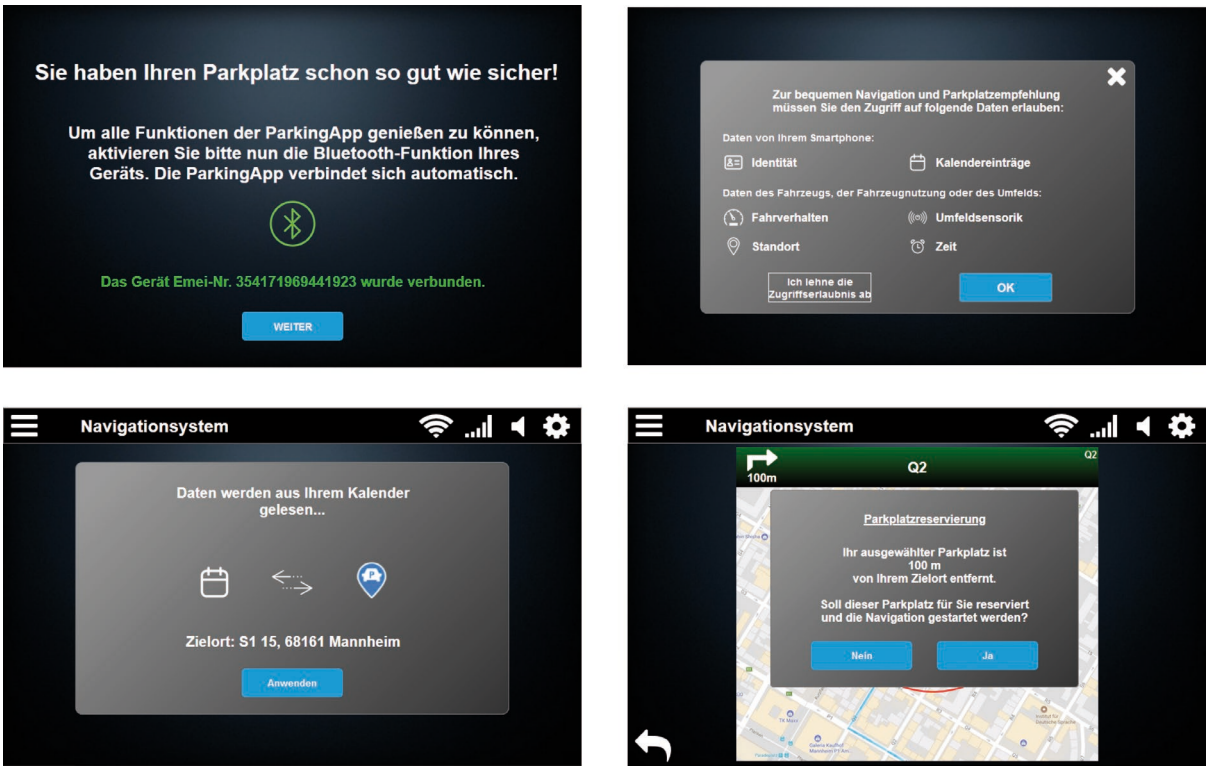


Abbildung 14. Übersicht über einzelne Bildschirme der ParkingApp. *Oben links*: Bestätigung der etablierten Bluetooth-Verbindung mit dem Smartphone. *Oben rechts*: Übersicht über die Datenpreisgabe in der Default-Version. *Unten links*: Übertragung der Kalendereinträge an die Parking App. *Unten rechts*: Parkplatz wurde für Reservierung ausgewählt.

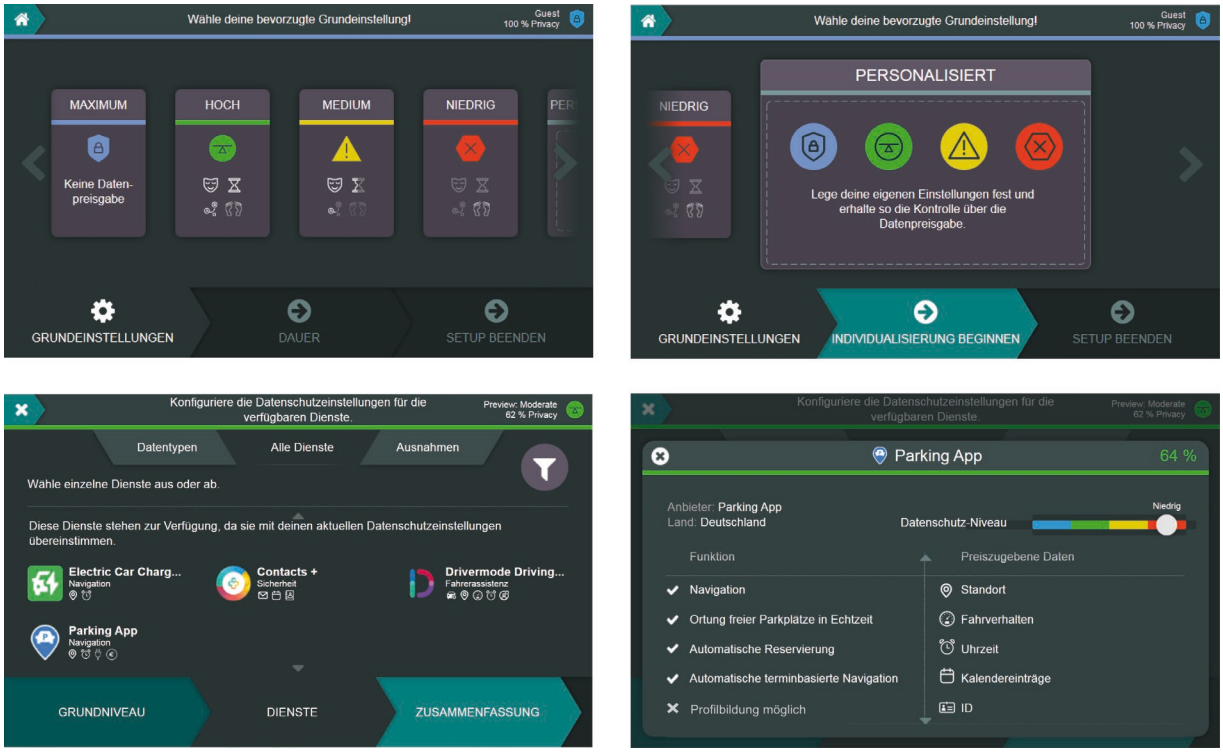


Abbildung 15. Übersicht über einzelne Seiten von PRICON. *Oben links*: Übersicht über die vordefinierten Datenschutzprofile. *Oben rechts*: Option zur Erstellung eines personalisierten Datenschutzprofils ist ausgewählt. *Unten links*: Zugriff auf die ParkingApp über PRICON. *Unten rechts*: Datenschutzeinstellungen für die ParkingApp mit einer Gegenüberstellung von verfügbaren Funktionen (links) und preiszugebenden Daten (rechts).

Wie in Kapitel 2.3.2 bereits aufgeführt stellt PRICON ein nutzendenzentriertes Kontrollmodul für eine selbstbestimmte Datenpreisgabe im vernetzten Automobil dar. Über die Auswahl von vordefinierten Datenschutzprofile oder das Erstellen eigener Datenschutzprofile können Nutzende das Ausmaß ihre informationelle Privatheit im Automobil selbst bestimmen. Für den Zweck dieser Studie wurde PRICON mit der ParkingApp verlinkt, sodass die Teilnehmenden nach der Einstellung einer von ihnen bevorzugten Datenpreisgabe mittels PRICON direkt zur entsprechenden Version (V1 bis V4) der ParkingApp weitergeleitet wurden. Abbildung 15 führt vier zentrale Seiten von PRICON auf.

Versuchsdurchführung. Der komplette Versuch dauerte ca. 90 Minuten und basierte auf einem within-subject Design mit dem zweistufigen Faktor tatsächliche Informationskontrolle (liegt nicht vor versus liegt vor). Abbildung 16 fasst den Versuchsablauf schematisch zusammen. Nachdem die Teilnehmenden ihre schriftliche Zustimmung zu der Teilnahme an der Studie gegeben hatten bekamen sie die Möglichkeit sich im Zuge einer kurzen Eingewöhnungsphase an das Fahrverhalten des Egofahrzeugs sowie die Simulatorumgebung zu gewöhnen. Hierzu wurde eine Fahrt von einer ländlichen in eine urbane Umgebung gewählt, die nach fünf Minuten durch den Versuchsleitenden beendet wurde.

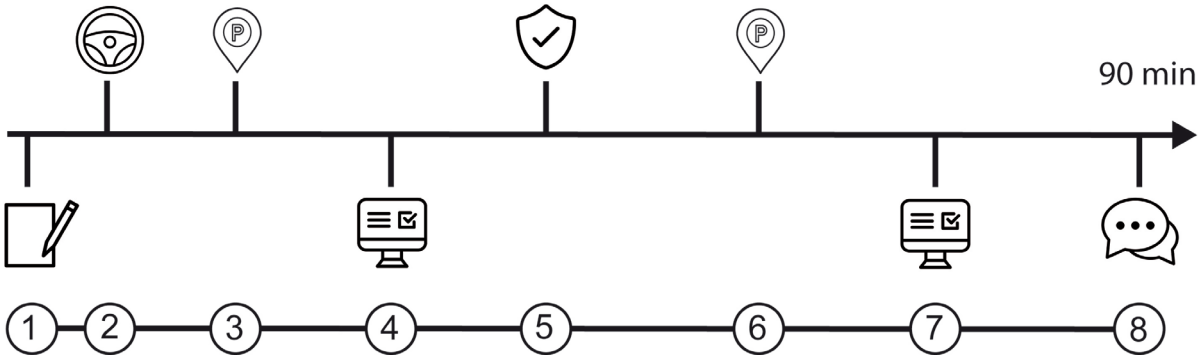


Abbildung 16. Schematischer Versuchsablauf. Einwilligung an Teilnahme (1) und Trainingsfahrt (2); Interaktion mit vernetzten Parkdienst ohne tatsächliche Kontrollmöglichkeit (3) und Ausfüllen des Online-Fragebogens (4); Ausübung einer tatsächlichen Informationskontrolle mittels PRICON (5); Interaktion mit vernetzten Parkdienst mit tatsächlicher Kontrollmöglichkeit (6) und Ausfüllen des Online-Fragebogens (7); Debriefing der Teilnehmenden (8).

Anschließend wurde die Parking-App auf dem Tablet im Fahrsimulator durch den Versuchsleitenden mittels Wizard-of-Oz-Technik freigeschaltet. Auf den ersten Bildschirmen der Parking-App wurden die Teilnehmenden in eine Coverstory eingeführt, die einen Produkttest eines neuen Parkdienstes in einem frühen Entwicklungsstatus ankündigte.

Der Test wurde in Kooperation mit der ConnCar AG durchgeführt, die auch gleichzeitig als datenempfangende Partei vorgestellt wurde. Die ConnCar AG wurde als Tochterunternehmen eines deutschen Automobilherstellers eingeführt, da eigene Benutzerbefragungen ergaben, dass das Vertrauen in Automobilhersteller durchschnittlich ausgeprägt ist, jedoch eine hohe Varianz aufzeigt (Walter & Abendroth, 2018). Anschließend wurden die Teilnehmenden gebeten sich vorzustellen, dass sie sich mit einer befreundeten Person in einem Café in Mannheim treffen würden. Dabei wurde Mannheim als Zielort ausgewählt, da es nah genug an Darmstadt liegt (ca. 50 km entfernt), um ein Treffen realistisch zu halten, jedoch gleichzeitig weit genug entfernt ist, sodass sich die Teilnehmenden wahrscheinlich in der Café- und Barszene Mannheims nur bedingt auskennen. Um einen kostenlosen Parkplatz einfach und komfortabel in der direkten Umgebung des Cafés zu finden, wurde den Teilnehmenden vorgeschlagen die neue ParkingApp zu benutzen. Hierzu konnten die Teilnehmenden über einen Start-Bildschirm des fahrzeugeigenen Betriebssystems innerhalb einer Übersicht über die verfügbaren Dienste auf die ParkingApp zugreifen. Als erstes mussten sich die Teilnehmenden in der ParkingApp registrieren. Im Zuge dessen wurden sie gebeten, die Bluetooth-Funktion ihres Smartphones zu aktivieren, damit sich der vernetzte Dienst mit dem Smartphone verbinden und auf die notwendigen Daten zugreifen könne. Auf einen Tastendruck des Versuchsleitenden hin erschien ein Bildschirm, der eine erfolgreiche Bluetooth-Verbindung vermeldete (Abbildung 14, oben links).

Um die ParkingApp zu nutzen, mussten die Teilnehmenden der Datenpreisgabe von insgesamt sechs Datenkategorien zustimmen (siehe Tabelle 5, erste Spalte). Das Einverständnis wurde mittels eines Bildschirms eingeholt, der an dem Design von Datenschutzmeldungen im Zuge der Installation von Applikationen in Android angelehnt war (siehe Abbildung 14, oben rechts). Wie bei der Nutzung von Smartphone-Applikationen wurden die Teilnehmenden mit einer Alles-oder-Nichts-Entscheidung konfrontiert: Die Preisgabe der angeforderten Daten ermöglichte die Nutzung der ParkingApp, während eine Ablehnung die Zugriffsverwehrung auf die ParkingApp zur Folge zu haben schien. Nachdem die Entscheidung der Datenpreisgabe gefällt wurde, wurden die Teilnehmenden (unabhängig von ihrer Entscheidung bezüglich der Datenpreisgabe) auf dem nächsten Bildschirm gebeten die Nutzung der ParkingApp fortzusetzen, um die Funktionen des vernetzten Dienstes im Zuge des Produkttests testen zu können. Unabhängig von ihren Entscheidungen bezüglich der Datenpreisgabe interagierten somit alle Teilnehmenden mit der gleichen Version der ParkingApp. Sobald die Entscheidung bezüglich der Datenpreisgabe gefällt wurde, simulierte eine Animation den Abruf von Kalendereinträgen von dem Smartphone der Teilnehmenden, sodass die Zieladresse des Cafés in Mannheim automatisch in die ParkingApp eingelesen werden konnte (Abbildung 14, unten links). Nun bekamen die Teilnehmenden mehrere Parkplätze in der direkten Umgebung des Zielortes vorgeschlagen, von denen sie einen auswählen und reservieren konnten (siehe Abbildung 14, unten rechts). Sobald die Teilnehmenden einen Parkplatz ausgewählt hatten, wurden sie von der ParkingApp auf einer Strecke von ungefähr fünf Minuten Fahrzeit zu diesem Parkplatz navigiert. Hierzu griff der Versuchsleitende wieder auf die Wizard-of-Oz-Technik zurück und starte mittels eines Tastendrucks die dynamische Nachverfolgung der Egoposition in der Navigationsanzeige der ParkingApp. Da sowohl die Streckenlänge als auch die vorgegebene Geschwindigkeit für die Teilstrecken bis zum Zielort bekannt waren, konnte die Geschwindigkeit der Egoposition in der Navigationsansicht vorab abgeschätzt und angepasst werden. Die Ampelschaltungen an jeder Kreuzung erforderten mehrere Haltevorgänge an roten Ampeln, sodass die gefahrene Route in mehrere kürzere Teilsegmente untereilt werden konnte, in denen leichte Abweichungen von der tatsächlichen Geschwindigkeit der Teilnehmenden nicht auffielen. Nachdem die Teilnehmenden am Zielparkplatz eingetroffen waren, wurden sie gebeten den Fahrsimulator zu verlassen und den Online-Fragebogen an einem Arbeitsplatz im Versuchsraum auszufüllen (siehe Abbildung 13). Der Online-Fragebogen umfasste die in Anhang A2 dargestellte Skalen.

Nachdem die Teilnehmenden wieder in den Fahrsimulator zurückgekehrt waren, hatten sie die Möglichkeit die Preisgabe von Daten im Zuge der Nutzung der ParkingApp zu kontrollieren. Hierzu wurde ihnen Zugriff auf PRICON gewährt. Im Zuge der Erstellung eines personalisierten Datenschutzprofils konnten die Teilnehmenden via PRICON auf die Datenschutzeinstellungen

der ParkingApp zugreifen und diese im Rahmen von vier vorgegebenen Stufen an ihre Präferenzen anpassen (siehe Abbildung 15). Je weniger Daten preisgegeben wurden, desto weniger Funktionen waren verfügbar. Tabelle 5 enthält eine Übersicht über die jeweils verfügbaren Funktionen und preiszugebenden Daten. Variante V1 entsprach dabei der Variante der ParkingApp, die zu Beginn des Experiments zum Einsatz kam.

Sobald die Teilnehmenden ihr bevorzugtes Datenschutzniveau für die ParkingApp gewählt hatten, konnten sie die ParkingApp nochmals auf der gleichen Strecke wie zu Beginn nutzen. Dabei war der verfügbare Funktionsumfang der ParkingApp von den mittels PRICON gewählten Datenschutzeinstellungen abhängig. Teilnehmende, die sich zur Preisgabe nur des Standortes entschieden (Tabelle 5, PRICON Level Maximal, ParkingApp Variante V4) hatte nur ein normales Navigationssystem zur Verfügung, während Teilnehmende, die zusätzlich noch das Fahrverhalten sowie die Uhrzeit preisgaben, freie Parkplätze angezeigt bekamen, ohne jedoch die Möglichkeit zu haben, diese zu reservieren (Tabelle 5, PRICON Level Hoch, ParkingApp Variante V3). Gaben Teilnehmende darüber hinaus auch ihre Identität preis, so konnten sie Parkplätze reservieren, verfügten jedoch über keinen automatischen Abruf von Zieladressen aus dem Kalender, sondern mussten diese manuell eingeben (Tabelle 5, PRICON Level Mittel, ParkingApp Variante V2). Diese Funktion war nur verfügbar, wenn alle Daten (inklusive der Kalendereinträge) preisgegeben wurden (Tabelle 5, PRICON Level Niedrig, ParkingApp Variante V1 (Default)).

Nach der Ankunft am Zielparkplatz der zweiten Fahrt füllten die Teilnehmenden wiederum den Online-Fragebogen aus. Dabei umfasste der zweite Fragebogen die gleichen Skalen wie der erste Fragebogen, enthielt darüber hinaus jedoch auch noch die demographischen Variablen. Zum Abschluss der Versuchsteilnahme wurden die Teilnehmenden über die Cover-Story sowie die Manipulationen (Wizard-of-Oz-Technik) aufgeklärt und erhielten die Aufwandsentschädigung. Keiner der Teilnehmenden gab an, eine der Manipulationen bemerkt zu haben.

Datenanalyse. Die erhobenen Daten aller Teilnehmenden wurden für die Datenanalyse überprüft und aufbereitet. Alle 116 Teilnehmenden erfüllten die Teilnahmekriterien ((korrigierte) Sehfähigkeit, Smartphone zur Hand, im Besitz eines gültigen Führerscheins mindestens Klasse B). Der komplette Datensatz wurde auf unvollständige Antworten überprüft, enthielt jedoch keine fehlenden Angaben. Negativ formulierte Items wurden invertiert, sodass alle Items einer Skala die gleiche Skalierungsrichtung besaßen. Somit konnte die komplette Stichprobe von 116 Teilnehmenden für die Datenanalyse verwendet werden.

Zur Beantwortung der Forschungsfrage 1 umfasste diese die Schätzung des postulierten Modells auf der Basis der *partial least squares (PLS)* Strukturgleichungsmodellierung mit der Software *SmartPLS 3.0* (Ringle et al., 2015). Die PLS Strukturgleichungsmodellierung wurde hier gewählt, da sie frei von Verteilungsannahmen und für komplexe Modelle besonders geeignet ist (Hair et al., 2011). Die Hypothesen der Forschungsfrage 2 wurden mittels nicht-parametrischen Paarvergleichen für verbundene Stichproben auf Basis des Wilcoxon-Rangsummen-Test überprüft. Hierzu wurden für alle Teilnehmenden und für jede Skala die Skalenmittelwerte für die Fragebogenerhebung vor (*pre*) und nach (*post*) PRICON mittels IBM SPSS Statistics 24 gebildet.

4.1.2. Ergebnisse

Die Teilnehmenden nahmen die Identität (M = 4,40; SD = 0,99) sowie Kalendereinträge (M = 4,48; SD = 0,84) als persönliche Daten wahr. Informationen über den Standort wurden tendenziell als eher persönlich bewertet (M = 3,90; SD = 1,04), während das Fahrverhalten weder als persönlich noch als unpersönlich betrachtet wurde (M = 3,09; SD = 1,14). Als vergleichsweise wenig persönlich wurden die Zeit (M = 2,66; SD = 1,29) sowie Daten der Umfeldsensorik aufgefasst (M = 2,75; SD = 1,21). Da nicht einzelne Daten, sondern das gesamte Datenpaket zur Nutzung des vernetzten Parkdienstes preisgegeben werden musste, wurde für jeden Teilnehmer ein Datensensibilitätsscore gebildet. Dieser entsprach der Summe aller Sensibilitätsbewertungen bezüglich der preiszugebenden Daten. Der Score konnte zwischen 6 und 30 Punkten variieren, mit einem Skalenmittel von 18 Punkten. Da der Median des Datensensibilitätsscores in dieser Stichprobe bei 21 Punkten lag, nahmen die Teilnehmenden das preiszugebende Datenpaket als sensibel wahr (Wilcoxon-Test gegen das Skalenmittel von 18 Punkten: Z = 7,26, $p < .001$). Entsprechend der intendierten Manipulation durch die Vorstellung der ConnCar AG als Tochterunternehmen eines deutschen Automobilherstellers vertrauten die Teilnehmenden der ConnCar AG (M = 2,56; SD = 0,85) geringfügig mehr als einem privaten Anbieter einer Applikation (M = 2,14; SD = 0,87), jedoch etwas weniger als einem Automobilhersteller (M = 2,81; SD = 0,94).

Im Folgenden werden die Ergebnisse der Modellevaluation im Zuge der Beantwortung von Forschungsfrage 1 sowie die nicht-parametrischen Paarvergleiche zur Überprüfung der Forschungsfrage 2 getrennt voneinander berichtet.

Forschungsfrage 1: Etablierung des Akzeptanzmodells für vernetzte Dienste. Zur Beantwortung der Forschungsfrage 1 wurden die Fragebogendaten nach der ersten Nutzung der ParkingApp, aber vor dem Einsatz von PRICON, herangezogen.

Die Information über preiszugebende Daten, ohne dabei eine tatsächliche Informationskontrolle zu haben, entspricht den Erfahrungen der Nutzenden im Kontext von Smartphone-basierten Applikationen (Beresford et al., 2011; Hang et al., 2012). Bevor das Strukturgleichungsmodell als solches geprüft wurde, wurde die Angemessenheit des Messmodells (operationalisiert durch den Fragebogen) mittels eines PLS faktoriellen Validitätstests überprüft. Der PLS Validitätstest ergab, dass alle standardisierten Faktorladungen signifikant höher waren als der Schwellwert von 0,70. Darüber hinaus überschritten alle durchschnittlich erfassten Varianzen (AVEs) den Grenzwert von 0,5, während die internen Konsistenzen aller latenten Konstrukte (d. h. die Modellfaktoren), erfasst mittels der kompositen Reliabilität ρ und Cronbach's α, größer als 0,7 waren (siehe Tabelle A2 im Anhang). Die diskriminante Validität des Messmodells wurde anhand des Fornell-Larcker-Kriteriums erfasst (Fornell & Larcker, 1981). Das Fornell-Larcker-Kriterium besagt, dass die quadrierte Wurzel eines jeden AVE eines latenten Konstrukts größer sein sollte als die Korrelation dieses Konstrukts mit anderen latenten Konstrukten. Wie Tabelle 6 zeigt, konnte für alle Konstrukte eine größere AVE als die Cross-Ladung auf andere latente Konstrukte gefunden werden, sodass das Fornell-Larcker-Kriterium erfüllt wurde.

Tabelle 6. Cross-Ladungen und durchschnittlich erfasste Varianzen (AVEs)

	ATT	BI	PU	PEOU	IC	PC	PR	TR	SN
ATT	0,829								
BI	0,802	0,896							
PU	0,635	0,543	0,817						
PEOU	0,327	0,258	0,532	0,815					
IC	0,258	0,349	0,194	0,033	0,900				
PC	-0,344	-0,377	-0,338	-0,194	-0,313	0,933			
PR	-0,326	-0,340	-0,286	-0,265	-0,330	0,838	0,918		
TR	0,514	0,416	0,413	0,157	0,301	-0,339	-0,355	0,810	
SN	0,739	0,763	0,536	0,225	0,295	-0,323	-0,304	0,475	0,849

Hinweis: Die AVEs sind auf der Diagonalen abgetragen. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Somit sprechen die Schätzungen der Modellparameter für eine hohe Validität und Reliabilität des Messmodells inklusive aller seiner Konstrukte.

Nachdem die Angemessenheit des Messmodells nachgewiesen wurde, kann das hypothetisierte Strukturgleichungsmodell getestet werden. Das aufgestellte Modell konnte $R_{Adjusted}$ = 69,9 Prozent der Varianz der Verhaltensintention, 70,4 Prozent der Varianz des wahrgenommenen Privatheitsrisikos sowie 41,1 Prozent der Varianz der Einstellung gegenüber der Nutzung erklären. Um die prädiktive Validität dieser drei latenten Variablen sicherzustellen, wurde der Stone-Geisser Q^2 Test angewandt. Alle Q^2-Werte waren signifikant größer als 0 (0,54, 0,57 und 0,27 für die Nutzungsintention, die wahrgenommenen Privatheitsbedenken sowie die Einstellung gegenüber der Nutzung), sodass eine geeignete prädiktive Validität für diese Zielvariablen angenommen werden kann.

Um die in den Hypothesen H1.1 bis H1.14 formulierten Pfadbeziehungen zwischen den einzelnen Konstrukten zu testen, wurde eine Bootstrap Analyse auf der Basis von 5000 Stichproben durchgeführt (Hair et al., 2011). Acht von 14 angenommenen Pfadbeziehungen konnten als signifikant nachgewiesen werden. H 1.1, die einen positiven Einfluss der wahrgenommenen Nützlichkeit auf die Einstellung gegenüber der Nutzung vorhersagte, wurde bestätigt (β = 0,61, t = 6,44, $p < .001$). Im Gegensatz dazu konnte kein signifikanter Effekt der wahrgenommenen Nützlichkeit auf die Nutzungsintention nachgewiesen werden (*H 1.2;* β = 0,02, t = 0,22, $p > .05$). Die wahrgenommene Einfachheit der Nutzung hatte einen signifikanten positiven Einfluss auf die wahrgenommene Nützlichkeit (*H 1.3*; β = 0,52, t = 4,62, $p < .001$), jedoch nicht auf die Einstellung gegenüber der Nutzung (*H 1.4;* β = -0,02, t = 0,30, $p > .05$). Im Einklang mit H 1.5 und H 1.6 konnte je ein signifikanter positiver Einfluss der Einstellung gegenüber der Nutzung (*H 1.5;* β = 0,52, t = 6,10, $p < .001$) sowie der sozialen Norm (*H 1.6*; β = 0,38, t = 5,11, $p < .001$) auf die Nutzungsintention nachgewiesen werden. Wie von H 1.7 und H 1.8 vorhergesagt, hatten die Privatheitsbedenken einen signifikanten positiven Einfluss auf das wahrgenommene Privatheitsrisiko (*H 1.7;* β = 0,80, t = 19,90, $p < .001$) sowie einen signifikanten negativen Einfluss auf das Vertrauen in den Anbieter (*H 1.8;* β = - 0,35, t = 4,24, $p < .001$). Im Gegensatz zu den Hypothesen H 1.9 und H 1.10 hatte das Vertrauen in den Anbieter jedoch weder einen signifikanten positiven Einfluss auf die Nutzungsintention (*H 1.9*; β = -0,07, t = 0,97, $p > .05$), noch einen signifikanten negativen Einfluss auf das wahrgenommenen Privatheitsrisiko (*H 1.10*; β = -0,07, t = 1,43, $p > .05$). Ebenso war der Einfluss des wahrgenommenen Privatheitsrisikos auf die Nutzungsintention nicht signifikant (*H 1.11;* β = -0,08, t = 1,22, $p > .05$).

Der Einfluss auf die Einstellung gegenüber der Nutzung war hingegen signifikant negativ (*H 1.12*; β = -0,16, t = 2,29, $p < .05$). Darüber hinaus konnte die angenommene Rolle der wahrgenommenen Informationskontrolle nur teilweise bestätigt werden. Während ein signifikanter negativer Einfluss der wahrgenommenen Informationskontrolle auf das wahrgenommene Privatheitsrisiko nicht nachgewiesen werden konnte (*H 1.13*; β = -0,06, t = 1,05, $p > .05$), war der negative Einfluss der wahrgenommenen Informationskontrolle auf die Privatheitsbedenken wie erwartet signifikant (*H 1.14*; β = -0,32, t = 3,78, $p < .001$). Tabelle 7 sowie Abbildung 17 fassen die Ergebnisse der PLS Strukturgleichungsmodellierung zusammen.

Tabelle 7. Ergebnisse der Prüfung der Hypothesen zu Forschungsfrage 1

Hypothese	*Beziehung*	β	t	p	
H 1.1	PU → ATT	0,612	6,44	<.001	H_0 abgelehnt
H 1.2	PU → BI	0,02	0,22	>.05	H_0 nicht abgelehnt
H 1.3	PEOU → PU	0,52	4,62	<.001	H_0 abgelehnt
H 1.4	PEOU → ATT	-0,02	0,30	>.05	H_0 nicht abgelehnt
H 1.5	ATT → BI	0,52	6,10	<.001	H_0 abgelehnt
H 1.6	SN → BI	0,38	5,11	<.001	H_0 abgelehnt
H 1.7	PC → PR	0,80	19,90	<.001	H_0 abgelehnt
H 1.8	PC → TR	-0,35	4,24	<.001	H_0 abgelehnt
H 1.9	TR → BI	-0,07	0,97	>.05	H_0 nicht abgelehnt
H 1.10	TR → PR	-0,07	1,43	>.05	H_0 nicht abgelehnt
H 1.11	PR → BI	-0,08	1,22	>.05	H_0 nicht abgelehnt
H 1.12	PR → ATT	-0,16	2,29	<.05	H_0 abgelehnt
H 1.13	IC → PR	-0,06	1,05	>.05	H_0 nicht abgelehnt
H 1.14	IC → PC	-0,31	3,78	<.001	H_0 abgelehnt

Hinweis: Signifikanzniveau ist α = .05. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

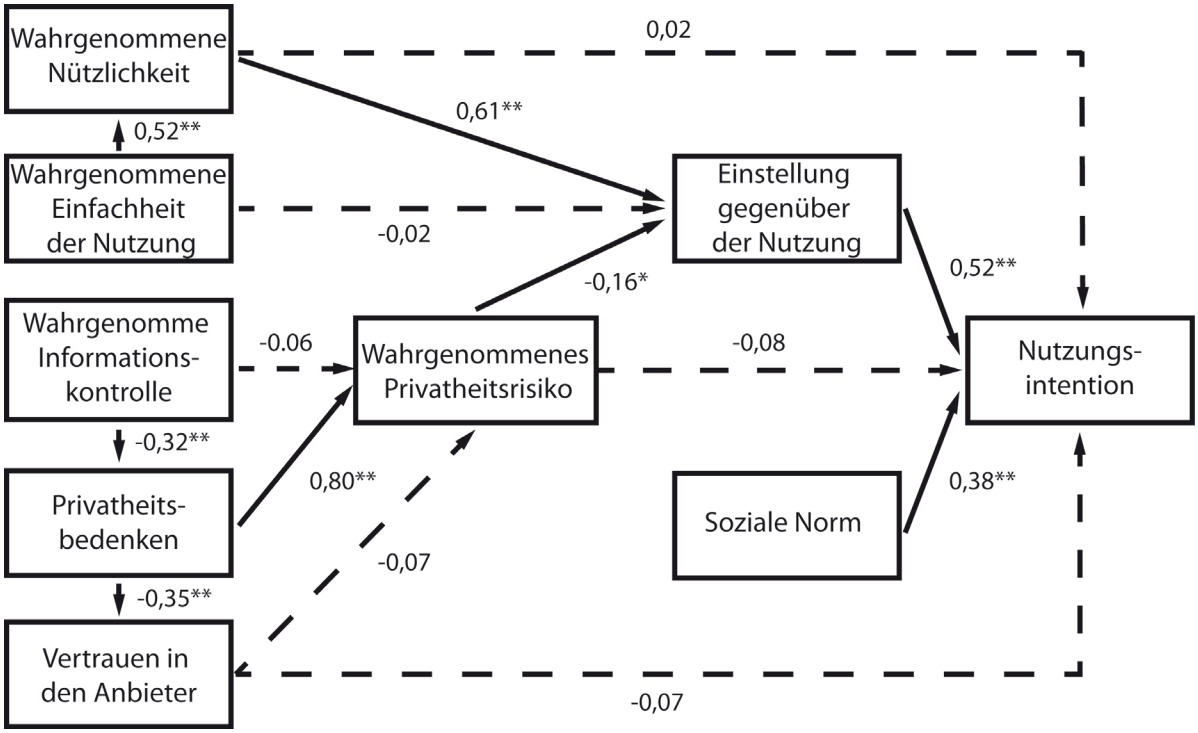


Abbildung 17. Ergebnisse der PLS Strukturgleichungsmodellierung zu den Hypothesen der Forschungsfrage 1. Dargestellt werden die Pfadkoeffizienten β. Gestrichelte Pfade kennzeichnen nicht signifikante Pfadbeziehungen.

In der bisherigen Analyse wurden alle Teilnehmenden unabhängig von ihrer Entscheidung bezüglich der initialen Preisgabe der angeforderten Daten für die Nutzung der ParkingApp berücksichtigt. Um zu überprüfen, ob sich solche Teilnehmende, die der Datenpreisgabe zugestimmt hatten (N = 103), von dem kompletten Sample unterscheiden, wurde das Strukturgleichungsmodell für dieses Subsample nochmals berechnet.

Wie in Tabelle A3 und Abbildung A1 zu sehen ist, konnte das Strukturgleichungsmodell der kompletten Stichprobe mit Ausnahme der Pfadbeziehung des wahrgenommenen Privatheitsrisikos zur Einstellung gegenüber der Nutzung sowie zur Nutzungsintention auch für die Teilnehmenden, die der Datenpreisgabe zugestimmt hatten, repliziert werden.

Forschungsfrage 2: Einfluss der Möglichkeit zur tatsächlichen Informationskontrolle auf die Akzeptanz von vernetzten Diensten im Automobil. Die Beantwortung der Hypothesen H 2.1 bis H 2.6 setzt einen Vergleich von Situationen ohne versus mit Informationskontrolle voraus. Entsprechend wurde Studie 1 auf der Basis eines within-subject Designs ausgelegt, sodass alle Teilnehmenden eine Situation ohne tatsächliche Informationskontrolle sowie eine Situation mit tatsächlicher Informationskontrolle durchliefen. Referenzpunkt und zugleich Operationalisierung der tatsächlichen Informationskontrolle war die Verfügbarkeit des Datenschutzinterfaces PRICON, mittels dessen die Teilnehmenden im zweiten Teil der Studie die ParkingApp

unter den von ihnen präferierten Datenpreisgabe nutzen konnten. Nach jeder Nutzung der ParkingApp wurden die Skalen zur Erfassung der im hypothetisierten Modell berücksichtigten Faktoren von den Teilnehmenden ausgefüllt, sodass jede Skala vor sowie nach der Möglichkeit zur tatsächlichen Informationskontrolle vorlag. Dieser *pre-post*-Vergleich ergab für die wahrgenommene Informationskontrolle eine höhere Ausprägung unter der Bedingung einer tatsächlichen Informationskontrolle (*H 2.1;* $Median_{pre}$ = 2, $Median_{post}$ = 3,33; Z = -7,66, $p < .001$). Das Vorliegen einer tatsächlichen Informationskontrolle hatte hingegen keinen signifikanten Einfluss auf das Vertrauen in den Anbieter (*H 2.2;* $Median_{pre}$ = 3,67, $Median_{post}$ = 3,67; Z = -1,93, p = .054). Die Privatheitsbedenken waren unter der Bedingung einer tatsächlichen Informationskontrolle geringer ($Median_{post}$ = 3,33) als ohne eine solche tatsächliche Informationskontrolle ($Median_{pre}$ = 4,00; *H 2.3;* Z = -4,81; $p < .001$). Entsprechend der Hypothese 2.4 war auch das wahrgenommene Privatheitsrisiko unter der Bedingung einer tatsächlichen Informationskontrolle geringer ($Median_{post}$ = 3,33) als ohne eine solche tatsächliche Informationskontrolle ($Median_{pre}$ = 3,67; Z = -4,21; $p < .001$). Die tatsächliche Informationskontrolle hatte auch auf die Einstellung gegenüber der Nutzung des vernetzten Parkdienstes einen signifikanten positiven Einfluss (*H 2.5;* Z = -2,34; $p < .05$). Dabei unterschieden sich die Mediane der Einstellung gegenüber der Nutzung des vernetzten Parkdienstes ohne ($Median_{pre}$ = 4,00) versus mit einer tatsächlichen Informationskontrolle ($Median_{post}$ = 4,00) nicht voneinander. Die Einstellung gegenüber der Nutzung unterschied sich jedoch dennoch über die Messzeitpunkte hinweg signifikant, da der Wilcoxon-Rangsummentest die beiden Messzeitpunkte auf Basis ihrer *Ränge* vergleicht. Dabei waren für N = 47 Teilnehmende bei einem *post minus pre* Vergleich die Ränge positiv (d.h. $Einstellung_{post} > Einstellung_{pre}$; $Rangsumme_{positiv}$ = 1677), während nur N = 24 Teilnehmende negative Ränge aufwiesen (d.h. $Einstellung_{post} < Einstellung_{pre}$; $Rangsumme_{negativ}$ = 879).

Tabelle 8. Ergebnisse der non-parametrischen Hypothesentests zur Beantwortung von Forschungsfrage 2.

	IC	TR	PC	PR	ATT	BI
$Median_{pre}$	2,00	3,67	4,00	3,67	4,00	3,67
$Median_{post}$	3,33	3,67	3,33	3,33	4,00	3,67
Z	-7,66	-1,93	-4,81	-4,21	-2,34	-1,75
p	< .001	.054	< .001	< .001	< .05	.08

Hinweis: Signifikanzniveau ist α = .05. . IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Bindungen lagen für 45 Teilnehmende vor (d.h. $Einstellung_{post} = Einstellung_{pre}$). Die Nutzungsintention bezüglich des vernetzten Parkdienstes unterschied sich hingegen nicht signifikant zwischen den Bedingungen ohne ($Median_{pre}$ =3,67) versus mit ($Median_{post}$ = 3,67) tatsächlicher Informationskontrolle (*H 2.6; Z* = -1,75, p = .08). Entsprechend unterschieden sich die Rangsummen für negative und positive Ränge kaum ($Rangsumme_{negativ}$ = 1129,5; $Rangsumme_{negativ}$ = 1796,5). Tabelle 8 fasst die Ergebnisse der non-parametrischen Hypothesentests zusammen.

In einer zusätzlichen explorativen Analyse wurde getestet, ob sich nicht nur die Ausprägungen der Modellfaktoren, sondern auch deren Pfadbeziehungen untereinander zwischen den Bedingungen ohne versus mit tatsächlicher Informationskontrolle unterscheiden. Hierzu wurde zuerst analog zu dem im Ergebnisteil zur Forschungsfrage 1 berichteten Vorgehen auch für die Nutzung des vernetzten Parkdienstes nach dem Einsatz von PRICON das postuliere Strukturgleichungsmodell mittels PLS berechnet. Die Ergebnisse hierzu sind im Anhang in Abbildung A2 zusammengefasst. Auf Basis der beiden Strukturgleichungsmodelle vor und nach dem Einsatz von PRICON wurde eine Multigruppenanalyse durchgeführt, um mögliche signifikante Unterschiede zwischen den Pfadkoeffizienten der jeweiligen Strukturgleichungsmodelle zu identifizieren (Hair et al., 2016). Die Multigruppenanalyse erfordert jedoch die Etablierung der Invarianz der Messmodelle (MICOM), die miteinander verglichen werden (Henseler et al., 2016). Dies umfasst daher die Sicherstellung, dass für die zu vergleichenden Modelle die gleichen Indikatoren (Items) sowie die gleiche Datenverarbeitung verwendet werden (Schritt 1; *Invarianz der Konfiguration*). In einem zweiten Schritt muss sichergestellt werden, dass die einzelnen Indikatoren über die zu vergleichenden Modelle hinweg einen vergleichbaren Einfluss auf die jeweiligen Konstrukte haben (*kompositionelle Invarianz)*. Während die Invarianz der Konfiguration durch die Auswahl der Items und Konstanz der Datenverarbeitung qualitativ sichergestellt werden muss, werden zur Sicherstellung der kompositionellen Invarianz die Indikatorkoeffizienten zwischen den beiden Modellen verglichen. Hierzu wird auf der Basis eines Permutationstests (hier: N = 5000) getestet, ob die Indikatorkoeffizienten signifikant von einer perfekten Korrelation (r = 1) abweichen. Besteht kein signifikanter Unterschied in den Indikatorkoeffizienten für ein bestimmtes Konstrukt zwischen den zu vergleichenden Modellen, d.h. sind die Korrelationen nicht signifikant geringer als r =1, kann von einer kompositionellen Invarianz ausgegangen werden. Bis auf die Nutzungsintention erfüllten alle Konstrukte die kompositionelle Invarianz (siehe Tabelle A4 im Anhang). Somit können alle Pfadbeziehungen, die die Nutzungsintention nicht miteinbeziehen, über die Bedingungen mit versus ohne tatsächliche Informationskontrolle miteinander verglichen werden. Wie Tabelle A5 im Anhang zeigt hatte die tatsächliche Informationskontrolle keinen Einfluss auf die Beziehungen zwischen den Modellfaktoren untereinander.

4.1.3. Diskussion

Studie 1 zielte sowohl auf die Etablierung eines Modells zur Erklärung der Nutzungsintention von vernetzten Diensten im Automobil unter Berücksichtigung der Datenpreisgabe (Forschungsfrage 1), als auch auf die Untersuchung des Einflusses einer tatsächlichen Informationskontrolle auf die Akzeptanz von vernetzten Diensten im Automobil (Forschungsfrage 2) ab.

Dabei konnte im Hinblick auf Forschungsfrage 1 die grundlegende angenommene Modellstruktur bestätigt werden. In Anlehnung an den privacy calculus (Dinev & Hart, 2006) kann das aufgestellte Modell als eine Detaillierung einer Kosten-Nutzen-Abwägung betrachtet werden. Während der obere, auf dem TAM (Davis, 1986) basierende Modellast den wahrgenommenen Nutzen repräsentiert, kann der untere privatheitsbezogene Ast als Abbildung der wahrgenommenen Kosten gesehen werden. Initial wurde in dieser Arbeit angenommen, dass sich diese Kosten-Nutzen-Abwägung direkt auf die Verhaltensintention auswirkt. Die Ergebnisse von Studie 1 zeigen jedoch, dass dieser Kosten-Nutzen-Abgleich bei Betrachtung der gesamten Stichprobe in der Einstellung gegenüber der Nutzung des vernetzten Dienstes resultiert. Ebenso wie in Lee (2009) werden daher bei der Entscheidung über die Nutzung eines vernetzten Dienstes im Automobil die privatheitsbezogenen Faktoren in eine affektive Bewertung der Nutzung eines solchen Dienstes integriert. Werden allerdings nur solche Personen betrachtet, die der Preisgabe der Daten zur Nutzung der vernetzten ParkingApp zustimmten, findet der Kosten-Nutzen-Abgleich wie erwartet auf Basis der Nutzungsintention statt. Wie bereits in Featherman et al. (2010) konnte auch hier gezeigt werden, dass datenpreisgebende Personen weniger gewillt sind ein Produkt oder Dienst zu nutzen, wenn ihre Bewertung der Wahrscheinlichkeit eines Kontrollverlusts über die preisgegebenen Daten hoch ist. Die Ergebnisse aus Studie 1 zeigen, dass neben den klassischen nutzenbezogenen Faktoren aus der Familie des TAM auch die Betrachtung der informationellen Privatheit bei der Nutzung von vernetzten Diensten im Automobil eine entscheidende Rolle spielt.

Während diese Makroperspektive eine Bestätigung des aufgestellten Modells vermuten lässt, zeigt die genauere Betrachtung, dass nicht alle angenommenen Pfadbeziehungen unterstützt wurden. Während die wahrgenommenen Vorteile, die mit der Nutzung des vernetzten Parkdienstes assoziiert sind, eine positive Einstellung gegenüber der Nutzung des vernetzten Parkdienstes förderten, hatten sie keinen direkten Einfluss auf die Intention diesen Dienst zu nutzen. Obwohl dies nicht den Vorhersagen des TAM entspricht, repliziert dieser Befund die Studie von Chen und Chen (2009) im Automobil. In vergleichbarer Weise konnte der Einfluss der Einfachheit der Nutzung auf die wahrgenommene Nützlichkeit bestätigt werden, während die Einstel-

lung gegenüber der Nutzung des vernetzten Parkdienstes nicht direkt durch die wahrgenommene Einfachheit der Nutzung beeinflusst wurde. Die Ergebnisse aus Studie 1 legen damit nahe, dass im Kontext von vernetzten Diensten im Automobil die Funktion, aber nicht der Aufwand, der zu deren Nutzung nötig ist, einer affektiven Bewertung unterliegt. Ergänzt werden diese Befunde durch den positiven Einfluss der sozialen Norm auf die Nutzungsintention. Darüber hinaus zogen die Teilnehmenden in Studie 1 bei der Bildung einer Nutzungsintention die Meinung der ihnen nahestehenden Personen bezüglich vernetzten Diensten im Automobil heran. Damit stehen die hiesigen Befunde im Einklang mit anderen Studien im automobilen Kontext (zum Beispiel Moons & Pelsmacker, 2012), die ebenfalls einen positiven Einfluss der sozialen Norm auf die Nutzungsintention beschrieben. Auch im privatheitsbezogenen Modellzweig konnte zwar die erwartete Grundstruktur, jedoch nicht jede Pfadbeziehung bestätigt werden. Motiviert durch die Befunde von Zhou (2012) wurde erwartet, dass die Privatheitsbedenken sowohl das wahrgenommene Privatheitsrisiko als auch das Vertrauen in den Anbieter beeinflussen. Das Vertrauen in den Anbieter sollte hingegen das wahrgenommene Privatheitsrisiko als auch die Intention zur Nutzung des vernetzten Parkdienstes direkt beeinflussen. Zwar konnten sowohl der positive Einfluss der Privatheitsbedenken auf das wahrgenommene Privatheitsrisiko ebenso wie der negative Einfluss der Privatheitsbedenken auf das Vertrauen in den Anbieter bestätigt werden. Wie bereits in mehreren Kontexten gezeigt werden konnte (Bansal et al., 2010; Zhou, 2012), sind auch Nutzenden von vernetzten Diensten im Automobil bezüglich des Umgangs mit den von ihnen preisgegebenen Daten besorgt. Nehmen diese Bedenken zu, kann das Vertrauen in den Anbieter darunter leiden, während das wahrgenommen Risiko für die eigene informationelle Privatheit im Zuge der Nutzung des vernetzten Dienstes zunimmt. Das Vertrauen in den Anbieter hatte hingegen weder einen Einfluss auf das wahrgenommene Privatheitsrisiko, noch auf die Nutzungsintention. Dies ist überraschend, da dieses Ergebnis im Widerspruch zu vorherigen Studien steht (Evjemo et al., 2018; Zhou, 2012). Eine mögliche Erklärung für diese Diskrepanz könnte in unterschiedlichen experimentellen Designs zwischen bisherigen Studien und Studie 1 dieser Arbeit liegen. Wie Gefen, Karahanna et al. (2003) zeigten reduziert die Erfahrung mit einem System oder einer Entität den Einfluss des Vertrauens. Falls Erfahrung mit einem System gesammelt wurden, nahm die Vorhersagekraft des Vertrauens für die Nutzung dieses Systems ab (Gefen, Karahanna et al., 2003). Während bisherige Studien vor allem auf der Präsentation von Text- oder Bildstimuli im Zuge von Online-Umfragen basierten, konnten die Teilnehmenden in dieser Studie tatsächliche Interaktionserfahrung mit dem vernetzten Parkdienst in der Simulationsumgebung erwerben. Daher könnte der Einfluss des Vertrauens in den Anbieter in dieser Studie durch den Einsatz des Fahrsimulators reduziert worden sein, da den Teilnehmenden somit tatsächliche Interaktionserfahrung vermittelt werden konnte. Motiviert durch die zentrale Rolle der Kontrolle in der Konzeption von Privatheit

(z. Bsp. Westin, 1967) sowie in Nutzendenbefragungen (Brell, Biermann et al., 2019) wurde die wahrgenommene Informationskontrolle in das Akzeptanzmodell für vernetzte Dienste im Automobil mit aufgenommen. Im Gegensatz zu Ando et al. (2016), die mögliche Einflussfaktoren auf die Nutzungsintention von Systemen im IoT-Kontext beleuchteten, konnte hier kein direkter Effekt der wahrgenommenen Informationskontrolle auf das wahrgenommene Privatheitsrisiko gefunden werden. Stattdessen wurde der Einfluss der wahrgenommenen Informationskontrolle auf das wahrgenommenen Privatheitsrisiko durch die Privatheitsbedenken vermittelt. Dieser Befund entspricht den Befunden vorheriger Studien, dass eine höhere wahrgenommenen Informationskontrolle zu einer Reduktion der Privatheitsbedenken führt (Culnan & Armstrong, 1999; Xu et al., 2011; Xu et al., 2013). Die Ergebnisse aus Studie 1 zeigen, dass die Wahrnehmung einer Informationskontrolle zwar keinen direkten, jedoch einen indirekten Einfluss auf das wahrgenommene Privatheitsrisiko hat. Die wahrgenommene Informationskontrolle führt zu einer Senkung der Privatheitsbedenken, was wiederum zu einem niedrigeren wahrgenommenen Privatheitsrisiko führt.

Obwohl nicht alle vermuteten Pfadbeziehungen bestätigt werden konnten, entsprechen die Ergebnisse aus Studie 1 der Grundarchitektur des aufgestellten Akzeptanzmodells für vernetzte Dienste im Automobil. Somit sollte die Reduzierung des wahrgenommenen Privatheitsrisikos ein Kernanliegen von Anbietern vernetzter Dienste im Automobil sein, sofern sie eine hohe Nutzungsintention bezüglich ihres Dienstes anstreben. Die hier bestätigten Modellstrukturen legen nahe, dass dabei direkt vertrauensstiftende Maßnahmen weniger Aussicht auf Erfolg versprechen als solche Maßnahmen, die die (wahrgenommene) Kontrolle über die Datenpreisgabe erhöhen.

Das sequenzielle Design von Studie 1 ermöglichte auch die Überprüfung von Forschungsfrage 2. Die Teilnehmenden interagierten zuerst mit der ParkingApp ohne eine Möglichkeit der Informationskontrolle (pre), um anschließend die Datenpreisgabe im Zuge der Nutzung der ParkingApp auf ihre Bedürfnisse anzupassen und nochmals mit der ParkingApp zu interagieren (post). Ein pre-post-Vergleich zeigte, dass die Möglichkeit zur tatsächlichen Informationskontrolle die wahrgenommene Informationskontrolle bei der Nutzung vernetzter Dienste im Automobil erhöht. Dabei steht dieser Befund im Einklang mit den Vorhersagen der Theory of Planned Behavior (Ajzen, 1985) und repliziert Studien im organisationalen Kontext (Wilson et al., 2015) sowie zur Ausgestaltung von Datenschutzerklärungen (Arcand et al., 2007). Die Ergebnisse von Arcand und Kollegen führten auch zu der Hypothese 2.2, die einen Anstieg des Vertrauens in den Anbieter durch die Bereitstellung der Möglichkeit einer tatsächlichen Informationskontrolle vorhersagte. Studie 1 konnte diese Annahme nicht bestätigen. Das Vertrauen in

den Anbieter war unter Vorliegen einer tatsächlichen Informationskontrolle trotz entsprechender Tendenzen nicht signifikant höher als ohne eine solche Kontrollmöglichkeit. Im Gegensatz zu Arcand et al. (2007) wurde in Studie 1 mit PRICON ein Kontrollmodul verwendet, dass nicht explizit mit dem Anbieter des vernetzten Dienstes in Zusammenhang stand. Die Teilnehmenden könnten daher die tatsächliche Kontrollmöglichkeit über die Datenpreisgabe nicht in dem Maße auf den Anbieter attribuiert haben, wie es in dem experimentell abweichenden Setting von Arcand und Kollegen der Fall war. Im Einklang mit der auf Wilson et al. (2015) basierenden Hypothese 2.3 waren die Privatheitsbedenken unter der Bedingung einer tatsächlichen Informationskontrolle geringer als ohne eine solche Kontrollmöglichkeit. Dies entspricht auch den Wirkmechanismen, die das in Forschungsfrage 1 aufgestellte Modell vorhersagt. Durch die erhöhte wahrgenommene Informationskontrolle, die durch die Möglichkeit der tatsächlichen Kontrolle über die Datenpreisgabe erzeugt wird, sinken die Privatheitsbedenken. Entsprechende Vorhersagen lassen sich auch aus der Studie von Xu et al. (2013) im Kontext von sozialen Netzwerken ableiten. Hajli und Lin (2016) sagten voraus, dass die Erhöhung der wahrgenommenen Informationskontrolle zu einer Absenkung des wahrgenommenen Privatheitsrisiko führen sollte (Hypothese 2.4). Obwohl in der Modellevaluation diese Beziehung für vernetzte Dienste hier nicht als signifikant nachgewiesen werden konnte (siehe Diskussion zu Forschungsfrage 1), war das wahrgenommene Privatheitsrisiko in der Tat geringer, wenn die Teilnehmenden die Möglichkeit einer tatsächlichen Informationskontrolle zur Verfügung hatten. In anderen Kontexten konnte bereits gezeigt werden, dass eine wahrgenommene Kontrolle risikobehaftete Verhaltensweisen begünstigt (Horswill & McKenna, 1999; Strickland et al., 1966) sowie die Risikobewertung beeinflusst (Du et al., 2006). Die hiesigen Ergebnisse legen nahe, dass die Erfahrung einer tatsächlichen Kontrolle über die Informationspreisgabe auch im Kontext von vernetzten Diensten die Bewertung des Risikos eines Daten(-kontroll-)verlusts senkt. In klassischen Modellen zur Prädiktion von Handlungen und Systemnutzungen wird die Einstellung als affektive und elaborierte Bewertung der Ausführung eines Verhaltens (zum Beispiel die Nutzung eines Systems) definiert (Fishbein & Ajzen, 1975). Im Kontext der Datenpreisgabe an eine Organisation konnte gezeigt werden, dass die wahrgenommene Kontrolle die Einstellung zu der Organisation positiv beeinflusst (Wilson et al., 2015). Ein entsprechender Effekt wurde auch für den Kontext vernetzter Dienste im Automobil erwartet (Hypothese H 2.5), der in Studie 1 bestätigt werden konnte. Ähnlich wie für Organisationen, die dem Schutz der Privatheit ihrer Kunden ein höheres Gewicht verleihen (Tsai et al., 2011), scheinen Nutzende von vernetzten Diensten im Automobil ebenfalls eine positivere Einstellung gegenüber der Interaktion mit dem Dienst zu haben, wenn dieser Dienst mit der Möglichkeit zur tatsächlichen Informationskontrolle verbunden wird. Dabei scheint es auszureichen, wenn diese Möglichkeit gegeben wird, selbst wenn dies in Form einer externen Applikation wie PRICON dargeboten wird. Während

die Einstellung gegenüber der Nutzung eines vernetzten Dienstes im Automobil durch das Vorliegen einer tatsächlichen Informationskontrolle positiv beeinflusst wurde, war dies für die Nutzungsintention nicht der Fall (Hypothese H 2.6). Wie bereits das oben diskutierte Modell für vernetzte Dienste zeigt, scheinen privatheitsrelevante Faktoren eher einen Einfluss auf die affektive und elaborierte Bewertung der Nutzung eines Dienstes zu haben anstatt die Nutzungsintention direkt zu beeinflussen. Dies spiegelt sich auch in dem Vergleich von Situationen mit versus ohne eine tatsächliche Informationskontrolle wieder. Die explorative Analyse der Pfadbeziehungen der Modelle für die Bedingungen mit versus ohne tatsächliche Informationskontrolle zeigte zudem, dass das Vorliegen der tatsächlichen Informationskontrolle zwar die Ausprägungen der betrachteten privatheitsrelevanten Faktoren beeinflusst, die Modellstruktur jedoch nicht verändert. Unabhängig von der Ausprägung der Möglichkeit zur Informationskontrolle hat das unter Forschungsfrage 1 aufgestellte Modell somit Gültigkeit für komfortbezogene vernetzte Dienste wie die hier eingesetzte ParkingApp.

Der Anspruch dieser Arbeit ist es jedoch, die Gültigkeit des Modells für vernetzte Dienste über verschiedene Kategorien der vernetzten Mehrwertdienste hinweg zu bewerten. Die Systematisierung nach Walter et al. (2020) schlägt hier die Kategorisierung von vernetzten Diensten im Automobil in komfortbezogene, effizienzbezogene und sicherheitsbezogene Dienste vor. Daher wurden noch zwei weitere Studien durchgeführt, die jeweils das Modell an einem effizienzbezogenen (Studie 2) und einem sicherheitsbezogenen Dienst (Studie 3) testeten.

4.2. Studie 2: Validierung des Modells am Beispiel eines effizienzbezogenen vernetzten Dienstes im Automobil

Befragungen von (potentiellen) Nutzenden vernetzter Mehrwertdienste im Automobil zeigen, dass neben Privatheitsbedenken vor allem der wahrgenommene Nutzen eine zentrale Rolle bei der Wahrnehmung eines solchen Dienstes spielt (Brell, Biermann et al., 2019; Schmidt et al., 2016; Schoettle & Sivak, 2014). Dabei wird effizienzbezogenen Diensten eine höhere Relevanz beigemessen als dass dies bei komfortbezogenen Diensten der Fall ist (Walter & Abendroth, 2018). Das hier postulierte Modell zur Erklärung der Nutzungsintention von vernetzten Diensten im Automobil sagt eine Abwägung zwischen den wahrgenommenen Vorteilen (der Nutzen eines vernetzten Dienstes) sowie den wahrgenommenen Kosten (die mit der Nutzung verbundene Datenpreisgabe) voraus. Während in Studie 1 ein solcher Abgleich auch strukturell nachgewiesen werden konnte, bleibt es offen, ob dies auch für effizienzbezogene Dienste gilt. Da diese eine höhere funktionale Wertschätzung seitens der Nutzenden erfahren, könnte sich die relative Relevanz zwischen wahrgenommenen Nutzen und wahrgenommenen Kosten zugunsten des Nutzens verschieben. Privatheitsrelevante Faktoren sollten dann entsprechend an Vorhersagekraft für die Nutzungsintention von vernetzten Diensten verlieren. Um die Aussagekraft

dieser Thesis in Bezug auf die Beantwortung von Forschungsfrage 1 über komfortbezogene Dienste hinaus zu erweitern, wurde mit Studie 2 eine online-basierte Studie durchgeführt, bei der ein effizienzbezogener Dienst im Fokus stand.

4.2.1. Methodik

Teilnehmende. 148 Personen füllten den Online-Fragebogen vollständig aus. Aufgrund von Qualitätskriterien wurden 42 Teilnehmende ausgeschlossen. Diese Kriterien waren der Besitz eines Führerscheins, das aufmerksame Betrachten eines Videos zur Vorstellung des vernetzten Dienstes (Details siehe weiterer Verlauf dieses Unterkapitels) sowie eine Bearbeitungsgeschwindigkeit, die auf eine sorgsame Bearbeitung schließen lässt. Das aufmerksame Betrachten des Videos wurde mit einer Kontrollfrage überprüft, die direkt nach dem Betrachten des Videos gestellt wurde. Die Teilnehmenden mussten in einer Mehrfachwahlaufgabe aus fünf vorgegebenen Datentypen die zwei Datentypen angegeben, die im Video vom vernetzten Automobil an die Infrastruktur gesendet wurde. Nur solche Teilnehmende, die ausschließlich die korrekten Datentypen benennen konnten, wurden in die weitere Analyse eingeschlossen. Die Bearbeitungsgeschwindigkeit wurde mit dem relativen Geschwindigkeitsindex (*englisch: relative speed index; RSI; Leiner, 2019*) erfasst. Der RSI setzt die individuelle Bearbeitungsgeschwindigkeit in Relation zu dem Median der Bearbeitungsgeschwindigkeit der Stichprobe. Hier wurden solche Teilnehmenden eingeschlossen, die einen RSI kleiner 2,2 aufwiesen. Insgesamt umfasste die für die Analyse verwendete Stichprobe somit 106 Teilnehmende (49 Frauen; M_{Alter} = 33,59 Jahre, SD_{Alter}= 13,54 Jahre). Neben dem Alter und dem Geschlecht wurden auch die durchschnittliche Häufigkeit der Smartphonenutzung sowie der Kenntnisstand bezüglich vernetzter Automobile vor der Teilnahme an der Studie abgefragt.

Nur 2 von 106 Teilnehmenden (1,89 %) berichteten kein Smartphone zu besitzen. 4 von 106 Teilnehmenden (3,77 %) benutzten ihr Smartphone nicht täglich. 71 von 106 Teilnehmenden (66,98 %) gaben an bereits vor der Studienteilnahme von vernetzten Automobilen gehört zu haben. Die teilnehmenden-bezogenen Informationen sind in Tabelle 9 zusammengefasst.

Tabelle 9. Zusammenfassung der Informationen über die Stichprobe in Studie 2.

Alter		Geschlecht		Kenntnis vor Studie		Smartphonenutzung	
M	33,59 J.	M	57	Ja	71	Täglich	100
SD	13,54 J.	W	49	Nein	35	Unregelmäßig / Nie	6

Die Teilnehmenden wurden im Umfeld der Technischen Universität Darmstadt, im privaten Umfeld des Autors, in Foren mit Automobilbezug sowie über die Plattform surveycircle.com rekrutiert. Die Studie wurde vom Ethikkomitee der Technischen Universität Darmstadt genehmigt. Entsprechend wurde von allen Teilnehmenden eine Einverständniserklärung bezüglich der Teilnahme an der Studie sowie der forschungsbezogenen Datenverarbeitung zu Beginn des Fragebogens eingeholt.

Materialien und Apparaturen. Der Online-Fragebogen wurde mittels soscisurvey.de programmiert und zur Verfügung gestellt. Der in Studie 2 eingesetzte Fragebogen basierte auf dem in Studie 1 verwendeten und validierten Fragebogen. Es wurden lediglich solche Items umformuliert, die einen direkten Bezug zu der in Studie 1 verwendeten Parkplatzapplikation aufwiesen. So wurde zum Beispiel das Item „Die Nutzung *der Parkplatzapplikation* vereinfacht *die Parkplatzsuche*." so umformuliert, dass ein Bezug zu vernetzten Diensten allgemein hergestellt wurde: „Die Nutzung *des vernetzten Dienstes* vereinfacht *meine Autofahrt*." Der angepasste Fragebogen kann in Tabelle A6 im Anhang nachvollzogen werden.

Der vernetzte Dienst. Da Studie 2 in Form einer Online-Befragung durchgeführt wurde, war es nicht möglich, in einer angemessen kurzen Bearbeitungszeit eine für den Versuchsleitenden nachvollziehbare beziehungsweise kontrollierbare Interkation mit dem vernetzten Dienst zu ermöglichen. Daher wurde ein animiertes Video erstellt, dass die Funktionen des vernetzten Dienstes *Green efficiency* in einer einfach verständlichen Art und Weise darstellt. Das 2,22 Minuten lange Video wurde mittels der Animationssoftware Animiz Animated Video Maker (Animiz Software Co. Ltd.) erstellt. *Green efficiency* wird in dem Video als vernetzter Mehrwertdienst vorgestellt, der den Fahrenden bei einer effizienten und klimafreundlichen Fahrweise unterstützt. Die ConnCar AG, ein Tochterunternehmen eines deutschen Automobilherstellers, wird wie in Studie 1 als Anbieter und somit datenempfangende Partie vorgestellt. Um den Zweck des vernetzten Dienstes aufzuzeigen, wird zuerst der Status Quo mit Staus und Stop-und-Go-Verkehr dargestellt, um anschließend die Wirkweise des effizienzbezogenen Dienstes darzustellen. Eine intelligente Vernetzung zwischen Verkehrsteilnehmern und der Infrastruktur wird aufgezeigt, wie mittels eines beidseitigen Datentransfers eine effiziente Fahrweise ermöglicht werden kann. In Abstimmung mit den sich auf der Route befindenden Ampelphasen können die nötigen Brems- und Beschleunigungsvorgänge so minimiert werden. In dem Video wird der Datentransfer zwischen einem Automobil und einer Ampelanlage animiert. Das Automobil sendet Informationen über den aktuellen Standort, das Fahrverhalten, die Geschwindigkeit sowie Brems- und Beschleunigungsvorgängen an die Ampelanlage und erhält im Gegenzug Informationen über die Dauer der jeweiligen Ampelphasen.

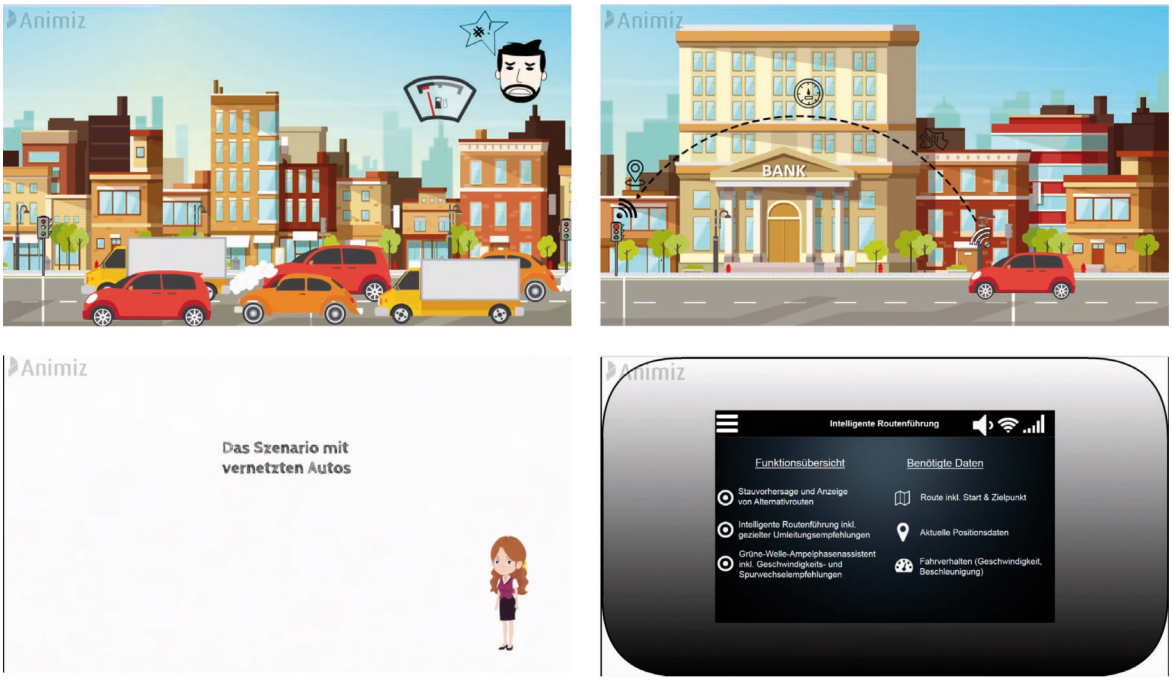


Abbildung 18. Screenshots des Videos zur Erklärung des vernetzten effizienzbezogenen Dienstes. *Oben links:* Auszug aus der Darstellung des Status-Quo. *Oben rechts*: Auszug aus der Funktionsweise des vernetzen Dienstes. *Unten links:* Darstellung der animierten Person, die durch das Video führt. *Unten rechts:* Gegenüberstellung der verfügbaren Funktionen und der preiszugebenen Daten.

So kann der vernetzte Dienst individuelle Empfehlungen für das Fahrverhalten geben, sodass Wartezeiten reduziert und der Verkehrsfluss erhöht werden können. Abschließend werden die verfügbaren Funktionen mit den benötigten Daten auf einem Bildschirm gegenübergestellt. Die Tonspur für dieses Video wurde von Pia Niesen eingesprochen. Abbildung 18 stellt vier Ausschnitte des Videos dar. Zur Überprüfung der Verständlichkeit des animierten Videos wurde selbiges sowohl wissenschaftlichen Mitarbeitern des Instituts für Arbeitswissenschaft im Rahmen eines institutsinternen Vortrags sowie Personen, die dem Forschungskontext fremd sind, zur Bewertung der Eingängigkeit in einem kurzen Interview vorgelegt. Alle beteiligten Personen gaben an, die Inhalte des Videos zu verstehen. In der Vortragsrunde am Institut für Arbeitswissenschaft wurde der Vorschlag geäußert, eine animierte Person, die durch das Video führt und einzelne Subsequenzen des Videos trennt (zum Beispiel die Erläuterung des Status Quo von der Vorstellung der Funktionsweise des vernetzten Dienstes; Abbildung 18 unten links), zu entfernen, da während der Anzeige der animierten Person kein Inhalt auf der Tonspur präsentiert wurde. Die forschungsfremden Personen hingegen begrüßten die inhaltliche Abtrennung. Daher wurde an dem Einsatz der animierten Person im Zuge des Videos festgehalten. Entsprechend der Stimme war auch die animierte Person weiblich.

Versuchsdurchführung. Die Teilnehmenden konnten über einen Link auf die Online-Umfrage zugreifen. Die Online-Umfrage war so ausgelegt, dass sie sowohl für die Bearbeitung an einem

Desktop-Rechner als auch einem mobilen Endgerät geeignet war. Auf der ersten Seite wurde der Zweck, die erwartete Bearbeitungsdauer des Fragebogens (10 min) sowie die durchführende Institution kurz beschrieben sowie die Einwilligung zur Datenerhebung unter den von der Ethikkommission empfohlenen und bewilligten Richtlinien eingeholt. Danach betrachteten die Teilnehmenden das oben beschriebene Video. Da der Inhalt des Videos für die Beantwortung der folgenden Fragen relevant war, wurde das aufmerksame Betrachten des Videos mittels einer inhaltlichen Kontrollfrage (siehe *Teilnehmende* zu Beginn dieses Unterkapitels) überprüft. Auf den folgenden Seiten wurden die Fragen des Akzeptierbarkeitsfragebogens angezeigt, wobei maximal zehn Fragen pro Seite angezeigt wurden. Der Online-Fragebogen schloss mit demographischen Fragen, Fragen zur wahrgenommenen Sensitivität der im Video preisgegebenen Daten (fünfstufige Skala mit den Endpunkten *nicht persönlich* und *persönlich*) und Fragen zum Vertrauen in unterschiedliche Entitäten wie die ConnCar AG ab (fünfstufige Skala mit den Endpunkten *stimme gar nicht zu* und *stimme voll zu* bezogen auf die Aussage „Ich vertraue [...] im Umgang mit meinen Daten."). Die durchschnittliche Bearbeitungsdauer der gültigen Fragebögen lag bei M = 8:35 min (SD = 3:47 min).

Datenanalyse. Die erhobenen Daten aller Teilnehmenden wurden wie in Kapitel 4.1.1 beschrieben für die Datenanalyse überprüft und aufbereitet. Für alle 106 Teilnehmenden wurden die negativ formulierten Items invertiert, sodass alle Items einer Skala die gleiche Skalierungsrichtung besaßen. Ebenso wie bereits in Studie 1 basierte die Schätzung des postulierten Modells auf der Basis der *partial least squares (PLS)* Strukturgleichungsmodellierung mit der Software *SmartPLS 3.0* (Ringle et al., 2015). Deskriptive Analysen wurden mit IBM SPSS Statistics 24 durchgeführt.

4.2.2. Ergebnisse

Ebenso wie in Studie 1 werden zuerst die wahrgenommene Sensitivität der preiszugebenden Daten sowie das Vertrauen in verschiedene datenempfangende Entitäten deskriptiv beschrieben. Anschließend wird die Modellvalidierung im Zuge der Beantwortung von Forschungsfrage 1 berichtet.

Die Teilnehmenden nahmen Informationen über den aktuellen Standort (M = 4,37; SD = 0,83) ebenso als persönlich wahr wie Routeninformationen (M = 4,02; SD = 1,00). Informationen zum Fahrverhalten wurden tendenziell persönlich wahrgenommen (M = 3,57; SD = 1,10). Da ebenso wie in Studie 1 nicht einzelne Daten, sondern das gesamte Datenpaket zur Nutzung des vernetzten Dienstes zur Steigerung der Verkehrseffizienz preisgegeben werden musste, wurde für jeden Teilnehmer ein Datensensibilitätsscore gebildet. Dieser entsprach der Summe aller Sensibilitätsbewertungen bezüglich der preiszugebenden Daten. Der Score konnte zwischen 3

und 15 Punkten variieren, mit einem Skalenmittel von 9 Punkten. Da der Median des Datensensibilitätsscores in dieser Stichprobe bei 12 Punkten lag, nahmen die Teilnehmenden das preiszugebende Datenpaket als sensibel wahr (Wilcoxon-Test gegen das Skalenmittel von 9 Punkten: $Z = 8{,}00$, $p < .001$). Entsprechend der intendierten Manipulation durch die Vorstellung der ConnCar AG als Tochterunternehmen eines deutschen Automobilherstellers vertrauten die Teilnehmenden der ConnCar AG ($M = 2{,}53$; $SD = 1{,}01$) stärker als einem privaten Anbieter einer Applikation ($M = 1{,}73$; $SD = 0{,}67$), jedoch etwas weniger als einem Automobilhersteller ($M = 2{,}71$; $SD = 2{,}02$).

Bevor das Strukturgleichungsmodell zur Validierung der Befunde aus Studie 1 als solches geprüft wurde, wurde die Angemessenheit des Messmodells (operationalisiert durch den Fragebogen) mittels eines faktoriellen PLS Validitätstests überprüft. Der PLS Validitätstest ergab, dass alle standardisierten Faktorladungen signifikant höher waren als der Schwellwert von 0,70. Darüber hinaus überschritten alle durchschnittlich erfassten Varianzen (AVEs) den Grenzwert von 0,5, während die interne Konsistenz aller latenten Konstrukte (d. h. die Modellfaktoren), erfasst mittels der kompositen Reliabilität ρ und Cronbach's α, größer als 0,7 war (siehe Tabelle A6 im Anhang).

Tabelle 10. Cross-Ladungen und durchschnittlich erfasste Varianzen (AVEs) für Studie 2

	ATT	BI	PU	PEOU	IC	PC	PR	TR	SN
ATT	0,860								
BI	0,853	0,961							
PU	0,784	0,755	0,828						
PEOU	0,393	0,522	0,333	0,820					
IC	0,330	0,425	0,391	0,246	0,891				
PC	-0,274	-0,388	-0,376	-0,223	-0,665	0,948			
PR	-0,351	-0,486	-0,478	-0,250	-0,725	0,905	0,935		
TR	0,463	0,627	0,537	0,462	0,627	-0,650	-0,725	0,840	
SN	0,757	0,816	0,637	0,450	0,413	-0,394	-0,499	0,515	0,880

Hinweis: Die AVEs sind auf der Diagonalen abgetragen. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Die diskriminante Validität des Messmodells wurde anhand des Fornell-Larcker-Kriteriums erfasst (Fornell & Larcker, 1981). Das Fornell-Larcker-Kriterium besagt, dass die quadrierte Wurzel eines jeden AVE eines latenten Konstrukts größer sein sollte als die Korrelation dieses Konstrukts mit anderen latenten Konstrukten. Wie Tabelle 10 zeigt, konnte für alle Konstrukte eine größere AVE als die Cross-Ladung auf andere latente Konstrukte gefunden werden, sodass das Fornell-Larcker-Kriterium erfüllt wurde. Somit sprechen die Schätzungen der Modellparameter für eine hohe Validität und Reliabilität des Messmodells inklusive aller seiner Konstrukte.

Nachdem die Angemessenheit des Messmodells nachgewiesen wurde, kann das hypothetisierte Strukturgleichungsmodell getestet werden. Das aufgestellte Modell konnte $R_{Adjusted}$ = 83,8 Prozent der Varianz der Verhaltensintention, 86,4 Prozent der Varianz des wahrgenommenen Privatheitsrisikos sowie 63,6 Prozent der Varianz der Einstellung gegenüber der Nutzung erklären. Um die prädiktive Validität dieser drei latenten Variablen sicherzustellen wurde der Stone-Geisser Q^2 Test angewandt. Alle Q^2-Werte waren signifikant größer als null (0,73, 0,71 und 0,43 für die Nutzungsintention, die wahrgenommenen Privatheitsbedenken sowie die Einstellung gegenüber der Nutzung), sodass eine geeignete prädiktive Validität für diese Zielvariablen angenommen werden kann.

Um die Befunde zu Forschungsfrage 1 aus Studie 1 an einem effizienzbezogenen vernetzten Mehrwertdienst im Automobil zu validieren, wurde wie in Studie 1 eine Bootstrap Analyse auf der Basis von 5000 Stichproben durchgeführt (Hair et al., 2011). Elf von 14 angenommenen Pfadbeziehungen konnten als signifikant nachgewiesen werden. H 1.1, die einen positiven Einfluss der wahrgenommenen Nützlichkeit auf die Einstellung gegenüber der Nutzung vorhersagte, wurde bestätigt (β = 0,77, t = 13,60, $p < .001$). Ebenso konnte ein signifikanter Effekt der wahrgenommenen Nützlichkeit auf die Nutzungsintention nachgewiesen werden (*H 1.2;* β = 0,21, t = 3,21, $p < .01$). Die wahrgenommene Einfachheit der Nutzung hatte einen signifikanten positiven Einfluss auf die wahrgenommene Nützlichkeit (*H 1.3*; β = 0,40, t = 4,27, $p < .001$), jedoch nicht auf die Einstellung gegenüber der Nutzung (*H 1.4;* β = 0,10, t = 1,35, $p > .05$). Im Einklang mit H 1.5 und H 1.6 konnte je ein signifikanter positiver Einfluss der Einstellung gegenüber der Nutzung (*H 1.5;* β = 0,36, t = 3,72, $p < .001$) sowie der sozialen Norm (*H 1.6*; β = 0,32, t = 4,74, $p < .001$) auf die Nutzungsintention nachgewiesen werden. Wie von H 1.7 und H 1.8 vorhergesagt, hatten die Privatheitsbedenken einen signifikanten positiven Einfluss auf das wahrgenommene Privatheitsrisiko (*H 1.7;* β = 0,68, t = 12,18, $p < .001$) sowie einen signifikanten negativen Einfluss auf das Vertrauen in den Anbieter (*H 1.8;* β = -0,65, t = 13,94, $p < .001$).

Tabelle 11. Ergebnisse der Prüfung der Hypothesen zu Forschungsfrage 1 am Beispiel eines effizienzbezogenen Dienstes.

Hypothese	*Beziehung*	β	t	p	
H 1.1	PU → ATT	0,77	13,60	<.001	H_0 abgelehnt
H 1.2	PU → BI	0,21	3,21	<.01	H_0 abgelehnt
H 1.3	PEOU → PU	0,40	4,27	<.001	H_0 abgelehnt
H 1.4	PEOU → ATT	0,10	1,35	>.05	H_0 nicht abgelehnt
H 1.5	ATT → BI	0,36	3,72	<.001	H_0 abgelehnt
H 1.6	SN → BI	0,32	4,74	<.001	H_0 abgelehnt
H 1.7	PC → PR	0,68	12,18	<.001	H_0 abgelehnt
H 1.8	PC → TR	-0,65	13,94	<.001	H_0 abgelehnt
H 1.9	TR → BI	0,21	2,74	<.01	H_0 abgelehnt
H 1.10	TR → PR	-0,19	3,29	<.01	H_0 abgelehnt
H 1.11	PR → BI	-0,04	0,73	>.05	H_0 nicht abgelehnt
H 1.12	PR → ATT	-0,01	0,02	>05	H_0 nicht abgelehnt
H 1.13	IC → PR	-0,16	3,43	<.01	H_0 abgelehnt
H 1.14	IC → PC	-0,67	12,13	<.001	H_0 abgelehnt

Hinweis: Signifikanzniveau ist α = .05. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Im Einklang mit den Hypothesen H 1.9 und H 1.10 hatte das Vertrauen in den Anbieter einen signifikanten positiven Einfluss auf die Nutzungsintention (*H 1.9*; $\beta = 0{,}21$, $t = 2{,}74$, $p < .01$) sowie einen signifikanten negativen Einfluss auf das wahrgenommenen Privatheitsrisiko (*H 1.10*; $\beta = -0{,}19$, $t = 3{,}29$, $p < .01$). Im Gegensatz dazu war weder der Einfluss des wahrgenommenen Privatheitsrisikos auf die Nutzungsintention (*H 1.11;* $\beta = 0{,}04$, $t = 0{,}73$, $p > .05$) noch der Einfluss auf die Einstellung gegenüber der Nutzung signifikant (*H 1.12*; $\beta = -0{,}01$, $t = 0{,}02$, $p > .05$).

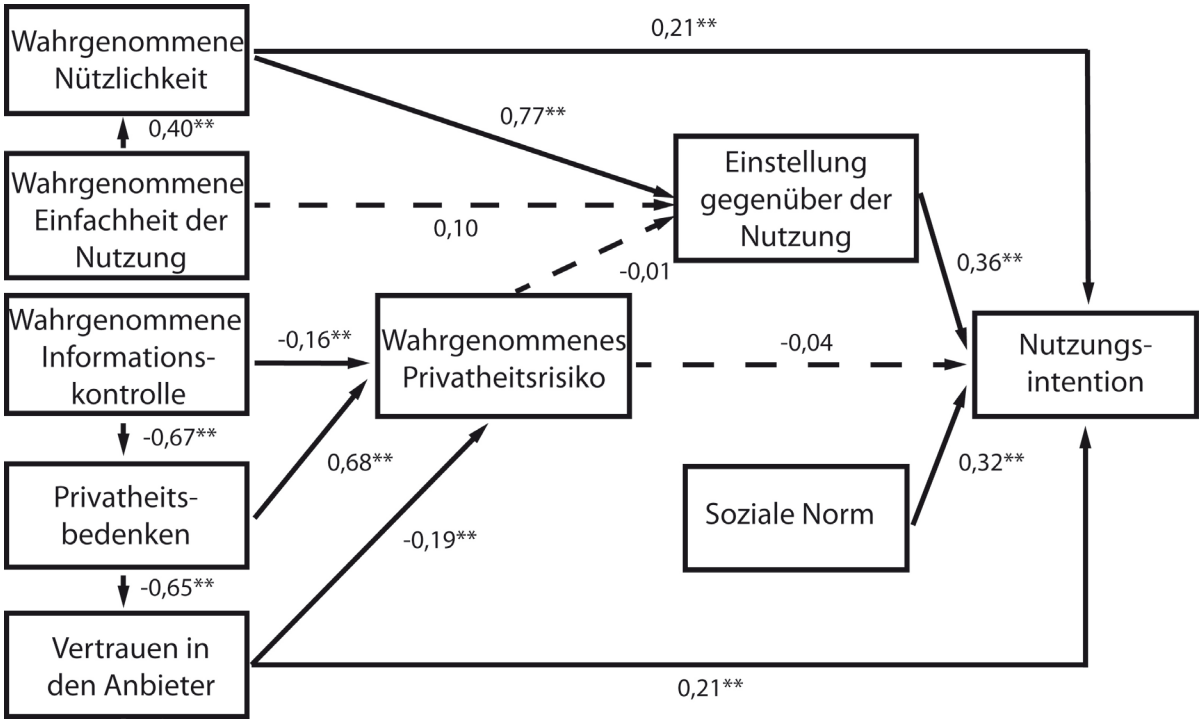


Abbildung 19. Ergebnisse der PLS Strukturgleichungsmodellierung zu den Hypothesen der Forschungsfrage 1. Dargestellt werden die Pfadkoeffizienten β. Gestrichelte Pfade kennzeichnen nicht signifikante Pfadbeziehungen.

Die vermutete Rolle der wahrgenommenen Informationskontrolle konnte hingegen bestätigt werden. Entsprechend den Hypothesen H 1.13 und H 1.14 hatte die wahrgenommenen Informationskontrolle einen signifikanten negativen Einfluss sowohl auf das wahrgenommene Privatheitsrisiko (β = -0,16, t = 3,43, p < .01) als auch auf die Privatheitsbedenken (β = -0,67, t = 12,13, p < .001). Tabelle 11 sowie Abbildung 19 fassen die Ergebnisse der PLS Strukturgleichungsmodellierung für vernetzte effizienzbezogene Dienste zusammen.

4.2.3. Diskussion

Studie 2 hatte zum Ziel das in Studie 1 etablierte Modell zu validieren und durch die Testung an einem effizienzbezogenen vernetzten Mehrwertdienst im Automobil einen Beitrag zur Erweiterung dessen Gültigkeitsanspruchs zu leisten. Um die Vergleichbarkeit der Szenarien sicherzustellen wurde wie am Beispiel eines komfortbezogenen vernetzten Mehrwertdienstes für das Automobil (Studie 1) auch hier die wahrgenommene Sensibilität der preiszugebenden Daten sowie das Vertrauen in die ConnCar AG als Unternehmen hinter dem vernetzten Dienst erfasst. Ebenso wie in Studie 1 nahmen die Teilnehmenden das preiszugebende Datenpaket als sensibel war. Das Vertrauen in die ConnCar AG war wie in der vorherigen Studie höher als das Vertrauen in einen App-Anbieter im Allgemeinen, jedoch niedriger als in einen Automobilhersteller.

Da Studie 2 als Replikation von Studie 1 in Bezug auf die Beantwortung der Forschungsfrage 1 gedacht ist, fokussiert sich die hiesige Diskussion auf Abweichungen von den Befunden in Studie 1. Die durch Studie 2 wiederholt bestätigten Pfadbeziehungen wurden bereits in Studie 1 diskutiert. Grundlegend konnte auch am Beispiel eines effizienzbezogenen vernetzten Mehrwertdienstes im Automobil eine Modellstruktur bestätigt werden, die als ein Kosten-Nutzen-Abgleich beschrieben werden kann. Allerdings unterscheidet sich das hiesige Modell im Sinne des Ortes dieses Abgleichs sowie des zentralen privatheitsbezogenen Faktors von dem Modell aus Studie 1. Während in Studie 1 das wahrgenommene Privatheitsrisiko den zentralen, privatheitsbezogenen Faktor darstellt, übernimmt in Studie 2 das Vertrauen in den Anbieter diese Rolle. Zwar hat auch das Modell in Studie 2 eine ausgesprochen hohe Varianzaufklärung für das wahrgenommene Privatheitsrisiko ($R_{adjusted}$ = 86,4 Prozent). Die hohe Varianzaufklärung für das wahrgenommene Privatheitsrisiko ist auch in dem direkten Einfluss der wahrgenommenen Informationskontrolle auf das wahrgenommene Privatheitsrisikos begründet, während der indirekte Einfluss, vermittelt über die Privatheitsbedenken, bestehen bleibt. Damit können in Studie 2 die Befunde von Ando et al. (2016) und Culnan und Armstrong (1999) in Bezug auf den Einfluss der wahrgenommenen Informationskontrolle repliziert werden. Trotz der hohen Varianzaufklärung hat das wahrgenommene Privatheitsrisiko jedoch selbst keine Vorhersagekraft mehr weder für die Einstellung gegenüber der Nutzung des effizienzbezogenen Dienstes noch für die Intention, diesen Dienst zu nutzen. Das wahrgenommene Privatheitsrisiko hat daher in Studie 2 eine deutlich geringere Relevanz in der Vorhersage der Nutzungsintention als noch in der ersten Studie.

Nutzendenbefragungen legen nahe, dass effizienzbezogene Funktionalitäten im vernetzten Automobil eine höhere Wertschätzung erfahren als komfortbezogene Funktionen (Brell, Biermann et al., 2019; Walter & Abendroth, 2018). In Folge dessen sollten funktionsbezogene Variablen in dem hiesigen Modell ein stärkeres Gewicht erfahren, während das wahrgenommene Privatheitsrisiko einen geringeren Einfluss hat. In der Tat ist dies hier zu beobachten. Im Gegensatz zu komfortbezogenen Diensten hat die wahrgenommene Nützlichkeit bei effizienzbezogenen Diensten einen direkten Einfluss auf die Nutzungsintention, während das wahrgenommene Privatheitsrisiko weder einen Einfluss auf die Einstellung gegenüber der Nutzung des Dienstes noch auf die Nutzungsintention hat. Anstelle des wahrgenommenen Privatheitsrisikos nimmt das Vertrauen in den Anbieter die zentrale Rolle unter den privatheitsbezogenen Modellfaktoren ein. Die hypothetisierten Pfadbeziehungen von dem Vertrauen in den Anbieter zu dem wahrgenommenen Privatheitsrisiko als auch zu der Nutzungsintention konnten in Studie 2 bestätigt werden, während beide in Studie 1 nicht bestätigt werden konnten. Ein Erklärungsansatz könnte lauten, dass je relevanter eine Funktion eines Dienstes ist, desto wichtiger sollte das

Vertrauen sein. Sollte die Funktion nicht verlässlich angeboten werden können ist der (wahrgenommene) Ausfall oder Schaden höher, wenn der entsprechenden Funktion eine höhere Relevanz beigemessen wurde. Dabei steht jedoch das Vertrauen in das System im Fokus (Ghazizadeh, Lee et al., 2012), während hier das Vertrauen in den Anbieter in Bezug im Umgang mit den erhobenen Daten intendiert ist. Obwohl jeweils ein Vertrauen in eine Entität erfasst wird, sind dies zwei zu unterscheidende Konstrukte, sodass Erklärungen mit Bezug auf das Vertrauen in das System nicht ohne Weiteres auf das Vertrauen in den Anbieter übertragen werden können. Auch wenn diese Studie diese Option nicht ausschließt, liegen bisher keine Forschungsergebnisse vor, die eine solche Übertragung rechtfertigen würden. Einen alternativen Erklärungsansatz liefern Gefen, Karahanna et al. (2003), die einen Einfluss der Nutzungserfahrung mit einem System auf die Vorhersagekraft des Vertrauens auf die Nutzungsintention beschreiben. Konnten Nutzende Erfahrungen mit einem System sammeln (wie zum Beispiel in Studie 1 der Fall), hat das Vertrauen eine geringere Vorhersagekraft, als dies der Fall für Bedingungen ohne Nutzungserfahrung ist. Die hier verwendete videobasierte Beschreibung des Szenarios gewährt den Teilnehmenden keine tatsächliche Nutzungserfahrung, sodass laut Gefen und Kollegen das Vertrauen an Relevanz gewinnen sollte. Im Vergleich zu Studie 1 ist dies hier in der Tat zu beobachten (siehe Abbildung 19 im Vergleich zu Abbildung 17). Zieht man die in Kapitel 2.4.1 eingeführte Unterscheidung zwischen Akzeptierbarkeit (Nutzungserfahrung liegt nicht vor) und Akzeptanz (Nutzungserfahrung liegt vor) hinzu, können die Unterschiede zwischen Studie 1 und Studie 2 auch aus der Perspektive der konzeptionellen Unterscheidung zwischen diesen beiden Konstrukten betrachtet werden. Unterschiede im experimentellen Design beider Studien führen dazu, dass in Studie 1 die Akzeptanz erfasst wurde, während in Studie 2 die Akzeptierbarkeit beschrieben wird. Die Abhängigkeit des Vertrauens von der Nutzungserfahrung nach Gefen, Karahanna et al. (2003) kann unter ebendieser Differenzierung von Akzeptierbarkeit und Akzeptanz betrachtet werden. Das Vertrauen in den Anbieter hat einen (größeren) Einfluss auf die Nutzungsintention, wenn die Akzeptierbarkeit eines Systems erfasst wird, während das Vertrauen in den Anbieter bei der Erfassung der Akzeptanz eine untergeordnete Rolle spielt.

Die Implikationen dieser Interpretation werden auch in der nächsten Studie aufgegriffen, in der die Anwendbarkeit des Modells für vernetzte Mehrwertdienste im Automobil am Beispiel eines sicherheitsbezogenen Dienstes geprüft wird. Da auch Studie 3 eine Online-Umfrage darstellt, die den Teilnehmenden keine tatsächliche Nutzungserfahrung bietet, wird ebenfalls die Akzeptierbarkeit erfasst. Sollte die oben aufgeführte Interpretation zutreffen, sollte auch in Studie 3 das Vertrauen in den Anbieter die Nutzungsintention vorhersagen.

4.3. Studie 3: Validierung des Modells am Beispiel eines sicherheitsbezogenen vernetzten Dienstes im Automobil

Ein Teilziel dieses Promotionsvorhabens ist die Entwicklung eines Akzeptanzmodells für vernetzte Dienste im Automobil, das den Aspekt der Privatheit berücksichtigt. Während die Studien 1 und 2 bereits jeweils einen repräsentativen Dienst für die Funktionsklassen Komfort und Effizienz entsprechend der Klassifikation nach Walter et al. (2020) betrachtet haben, steht die Anwendung des Modells auf einen sicherheitsbezogenen Dienst noch aus. Sicherheit ist dabei die Funktionsklasse, die seitens der Nutzenden die höchste Wertschätzung erfährt (Brell, Biermann et al., 2019; Walter & Abendroth, 2018). Basierend auf den Ergebnissen der Studien 1 und 2 sowie unter Berücksichtigung der funktionsbezogenen Präferenzhierarchie sollte sich die Relevanz der Sicherheit in einer prominenten Rolle des wahrgenommenen Nutzens wiederspiegeln. In Anbetracht des in Studie 2 diskutierten Einflusses der Nutzungserfahrung auf die Rolle des Vertrauens (Gefen, Karahanna et al., 2003) sollte auch in Studie 3 das Vertrauen in den Anbieter eine Vorhersagekraft auf die Nutzungsintention des sicherheitsbezogenen Dienstes haben. Wie Studie 2 wird auch Studie 3 als Online-Umfrage durchgeführt, die eine tatsächliche Anwendungsmöglichkeit entbehrt. Während Gefen und Kollegen die Nutzungserfahrung als entscheidend für den Einfluss des Vertrauens in den Anbieter betrachten, kann die Nutzungserfahrung auch als eine spezielle Form der Information über das zu nutzende System und dessen Anbieter betrachtet werden. Entsprechend könnte nicht nur die Nutzungserfahrung, sondern das Vorliegen von Informationen über den Anbieter und das System an sich bereits die Rolle des Vertrauens beeinflussen. Daher wird in Studie 3 die Verfügbarkeit der Identität des Dienstanbieters über die Teilnehmenden hinweg manipuliert. Sollte nicht nur das Vorliegen der Nutzungserfahrung, sondern bereits das Vorliegen von Informationen bezüglich des Dienstanbieters für die prädiktive Rolle des Vertrauens in den Anbieter entscheidend sein, so sollte das Vertrauen in den Anbieter im Sinne des weitergedachten Ansatzes von Gefen, Karahanna et al. (2003) für diejenigen Teilnehmenden, die keine Informationen über die Identität des Dienstanbieters zur Verfügung haben, eine größere prädiktive Rolle spielen

4.3.1. Methodik

Teilnehmende. Die Datenerhebung für Studie 3 wurde in Kooperation mit einem Panelanbieter durchgeführt. 202 Personen füllten den Online-Fragebogen vollständig aus. Insgesamt riefen 413 Personen den Fragebogen auf. 21 Personen lehnten die durch ein Votum des Ethikrats der TU Darmstadt genehmigten Datenschutzbestimmungen ab, 23 Personen waren nicht im Besitz eines Führerscheins der Klasse B oder höher. Da wie in Studie 2 der vernetzte Mehrwertdienst in Form eines Videos vorgestellt wurde, wurde auch in Studie 3 das aufmerksame Betrachten des Videos überprüft. Dies geschah mittels einer nachgelagerten Testfrage bezüglich der im

Video kommunizierten Datenpreisgabe. 152 Personen konnten die preisgegebenen Daten nicht korrekt benennen, sodass für sie die Umfrage direkt beendet wurde (Screen-Out). Eine Person brach die Bearbeitung in der Mitte des Fragebogens ab. Die übrigen 202 Personen waren im Besitz eines Führerscheins der Klasse B oder höher, hatten das Video zur Einführung des vernetzten Dienstes aufmerksam verfolgt und waren mit der Datenerhebung einverstanden.

Im Nachhinein wurden drei weitere Personen aufgrund einer im Vergleich zum Median der Stichprobe verdächtig schnellen Bearbeitungszeit (erfasst über den RSI < 2; Leiner, 2019) ausgeschlossen, sodass 199 Personen (99 Frauen; M_{Alter} = 46,20 Jahre, SD_{Alter}= 14,86 Jahre) in die Datenauswertung einflossen. Neben dem Alter und dem Geschlecht wurden auch die durchschnittliche Smartphonenutzung sowie der Kenntnisstand bezüglich vernetzter Automobile vor der Teilnahme an der Studie abgefragt. 13 von 199 Teilnehmenden (6,5 %) berichteten kein Smartphone zu besitzen. 6 von 199 Teilnehmenden (3,0 %) benutzten ihr Smartphone nicht täglich. 131 von 199 Teilnehmenden (65,8 %) gaben an bereits vor der Studienteilnahme von vernetzten Automobilen gehört zu haben. Die teilnehmenden-bezogenen Informationen sind in Tabelle 12 zusammengefasst. Die Studie wurde vom Ethikkomitee der Technischen Universität Darmstadt genehmigt. Alle Teilnehmenden wurden über den Panelanbieter für die Teilnahme an der Studie entlohnt.

Tabelle 12. Zusammenfassung der Informationen über die Stichprobe in Studie 3.

Alter		Geschlecht		Kenntnis vor Studie		Smartphonenutzung	
M	46,20 J.	M	100	Ja	131	Täglich	180
SD	14,86 J.	W	99	Nein	68	Unregelmäßig / Nie	19

Materialien und Apparaturen. Der Online-Fragebogen wurde mittels soscisurvey.de programmiert und zur Verfügung gestellt. Der in Studie 3 eingesetzte Fragebogen basierte auf dem in Studie 2 verwendeten und in Studie 1 validierten Fragebogen. Ähnlich wie bereits für Studie 2 wurden lediglich solche Items umformuliert, die einen direkten Bezug zu dem in Studie 2 verwendeten effizienzbezogenen Mehrwertdienst aufwiesen. Darüber hinaus wurden ergänzend zu den bestehenden Items für die wahrgenommene Nützlichkeit zwei weitere Items aufgenommen. Der angepasste Fragebogen kann in Tabelle A8 im Anhang nachvollzogen werden.

Der vernetzte Dienst. Wie in Studie 2 wurde auch für diese Online-Befragung ein animiertes Video erstellt, das die Funktionen eines vernetzten sicherheitsbezogenen Dienstes in einer einfach verständlichen Art und Weise darstellt. Das 2,13 Minuten lange Video wurde mittels der

Animationssoftware Adobe Animate (Adobe Inc.) erstellt und mehrfach an kleinen Stichproben (jeweils N = 5) evaluiert (Welling, 2019). Zu Beginn des Videos wird das nicht vernetzte Automobil mit einem vernetzten Automobil verglichen, sodass ein allgemeines Verständnis bezüglich des vernetzten Automobils sichergestellt wird. Anschließend werden die sicherheitsbezogenen Funktionen des vernetzten Dienstes in drei Schritten vorgestellt. Zuerst wird die Fernwartung zur Sicherstellung eines sicheren Fahrzeugzustands vorgestellt.

In einem zweiten Schritt wird ein automatisches Notrufsystem hinzugefügt, das an dem in der Europäischen Union vorgeschriebenen *eCall*-System (Verordnung (EU) 2015/758, 2015/Deutsch) angelehnt ist. In dem dritten Schritt wird der Funktionsumfang durch die Einführung der gesundheitsbezogenen Fahrerüberwachung vervollständigt. Falls der Fahrer während der Fahrt gesundheitliche Probleme bekommt, benachrichtigt der sicherheitsbezogene Dienst von selbst einen Notdienst. Wie der Funktionsumfang baut sich auch das Datenpaket, das im Zuge der Nutzung dieses Dienstes preisgegeben werden muss, über die drei Schritte auf. Mit der Einführung der dritten Funktionsstufe ist das Datenpaket komplett und umfasst die Preisgabe der Fahrzeugidentifikationsnummer, den Fahrzeugzustand, die Zeit, die Position sowie Augenbewegungen und die Herzschlagfrequenz.

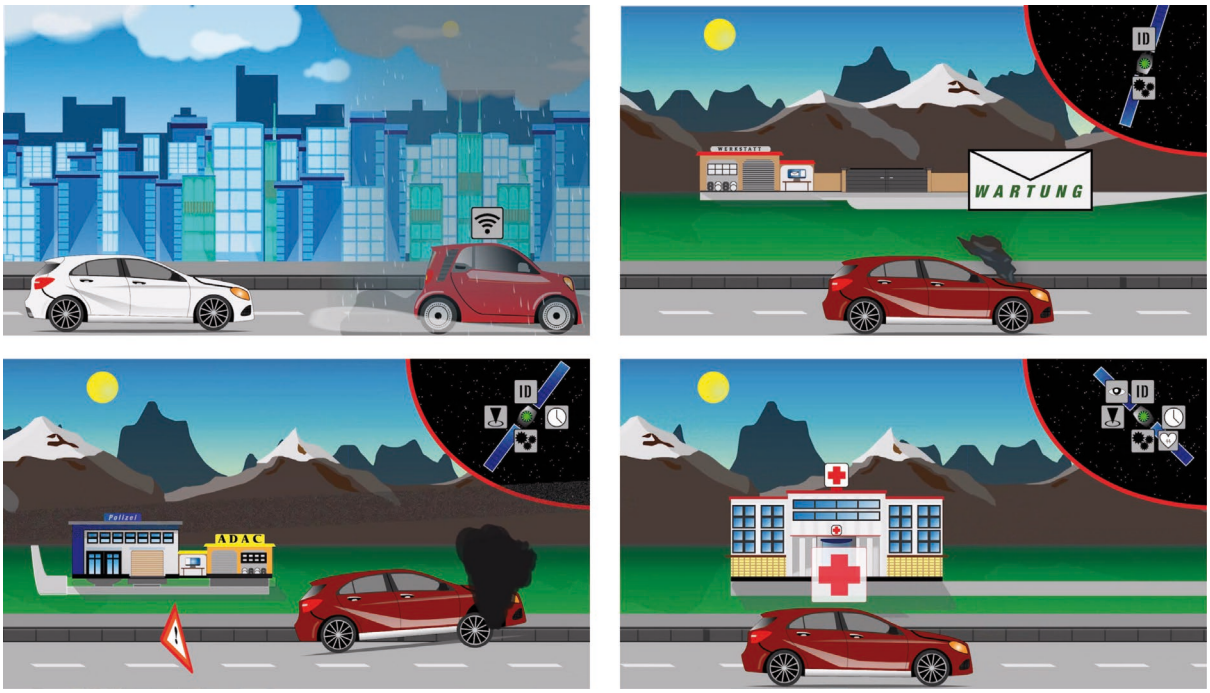


Abbildung 20. Ausschnitte aus dem Video zur Vorstellung des sicherheitsbezogenen Dienstes in Studie 3. *Oben links:* Das vernetzte Automobil wir im Allgemeinen vorgestellt. *Oben rechts:* Im ersten Schritt wird die Fernwartung eingeführt. *Unten links:* Im zweiten Schritt wird der automatische Notruf im Falle eines Unfalls vorgestellt. *Unten rechts:* Im dritten Schritt wird die gesundheitsbezogene Fahrerüberwachung präsentiert. Die Datenpreisgabe ist im oberen rechten Eck dargestellt und umfasst nun das komplette Datenpaket.

Die Tonspur wurde von Alexander Welling eingesprochen. Abbildung 20 zeigt vier Ausschnitte aus dem animierten Video.

Versuchsdurchführung. Die Teilnehmenden konnten über einen Link auf die Online-Umfrage zugreifen. Die Online-Umfrage war so ausgelegt, dass sie sowohl für die Bearbeitung an einem Desktop-Rechner als auch einem mobilen Endgerät geeignet war. Auf der ersten Seit wurde der Zweck, die erwartete Bearbeitungsdauer des Fragebogens (10 min) sowie die durchführende Institution kurz beschrieben sowie die Einwilligung zur Datenerhebung unter den von der Ethikkommission empfohlenen und bewilligten Richtlinien eingeholt. Personen, die nicht ihre Einwilligung gaben, wurden über einen Screen-Out-Link direkt zum Panelanbieter zurückgeleitet. Danach folgte eine weitere Filterfrage, die den Besitz eines Führerscheins sicherstellte. Nur solche Personen, die die Frage nach dem Führerscheinbesitz bejahten, konnten die Umfrage fortführen. Anschließend betrachteten die verbliebenen Teilnehmenden das oben beschriebene Video. Da der Inhalt des Videos für die Beantwortung der folgenden Fragen relevant war, wurde das aufmerksame Betrachten des Videos mittels einer inhaltlichen Kontrollfrage überprüft. Der Hälfte der Teilnehmenden wurde im Nachgang des Videos die ConnCar AG als datenempfangende Entität in einem Satz hervorgehoben. Die andere Hälfte sah diesen Hinweis nicht. Die Zuweisung der Teilnehmenden zu den jeweiligen Gruppen war randomisiert. Um sicherzustellen, dass sich die beiden Gruppen nicht voneinander unterscheiden und die Datenauswertung auf Basis der kompletten Stichprobe durchgeführt werden kann, wird die Zulässigkeit der Vermischung beider Bedingungen in Kapitel 4.3.2 überprüft. Nur solche Teilnehmenden füllten den sich anschließenden Fragebogen aus, die diejenigen Daten auswählen konnten, die ausschließlich für Schritt drei des Videos benötigt wurden (richtig: Augenbewegungen und Herzschlagrate). Auf den folgenden Seiten wurden die Fragen des Akzeptierbarkeitsfragebogens präsentiert, wobei maximal zehn Fragen pro Seite angezeigt wurden. Der Online-Fragebogen schloss mit demographischen Fragen, Fragen zur wahrgenommenen Sensitivität der im Video preisgegebenen Daten (fünfstufige Skala mit den Endpunkten *nicht persönlich* und *persönlich*) und Fragen zum Vertrauen in unterschiedliche Entitäten wie ein Automobilhersteller ab (fünfstufige Skala mit den Endpunkten *stimme gar nicht zu* und *stimme voll zu,* bezogen auf die Aussage „Ich vertraue [...] im Umgang mit meinen Daten.“). Die durchschnittliche Bearbeitungsdauer der gültigen Fragebögen lag bei M = 7:57 min (SD = 1:52 min).

Datenanalyse. Die erhobenen Daten aller Teilnehmenden wurden wie in den vorangegangenen Studien für die Datenanalyse überprüft und aufbereitet. Für alle 199 Teilnehmenden wurden die negativ formulierte Items invertiert, sodass alle Items einer Skala die gleiche Skalierungsrichtung besaßen. Ebenso wie bereits in den vorangegangenen Studien basierte die Datenana-

lyse die Schätzung des postulierten Modells auf der Basis der *partial least squares (PLS)* Strukturgleichungsmodellierung mit der Software *SmartPLS 3.0* (Ringle et al., 2015). Deskriptive Analysen wurden mit IBM SPSS Statistics 24 durchgeführt.

4.3.2. Ergebnisse

Aufgrund der experimentellen Manipulation im Zuge des Fragebogens für Studie 3 wurde es notwendig zu überprüfen, ob die beiden Gruppen (expliziter Hinweis auf Datenempfänger vorhanden vs. nicht vorhanden) zu einer Gesamtstichprobe zusammengefügt werden können. Hierzu wurde das in Studie 1 bereits beschriebene Verfahren zur Etablierung der Invarianz der Messmodelle (MICOM) herangezogen. Während in Studie 1 lediglich das Ziel war, die Zulässigkeit eines Vergleiches von Gruppen auf der Basis des gleichen Strukturgleichungsmodells sicherzustellen, muss hier die Zulässigkeit der Zusammenführung (Pooling) von Gruppen zu einer Gesamtstichprobe getestet werden. In Kapitel 4.1.2 wurden hierzu bereits die ersten beiden Stufen *Invarianz der Konfiguration* sowie *kompositionelle Invarianz* beschrieben. Für den Zweck des Poolings muss jedoch die *komplette Invarianz des Messmodells* nachgewiesen werden, was neben den ersten beiden Stufen auch die *Etablierung gleicher Mittelwerte und Varianzen* umfasst (Henseler et al., 2016). Während die Invarianz der Konfiguration durch die Beibehaltung des identischen Messmodells sowie der gleichen Parameter für die Datenauswertung sichergestellt wird, können die Stufen 2 und 3 der MICOM empirisch getestet werden. Wie zur Erfassung der kompositionellen Invarianz (siehe Kapitel 4.1.2) wird auch zur Etablierung gleicher Mittelwerte und Varianzen auf einen Permutationstest zurückgegriffen. In N = 5000 Durchläufen werden durch randomisierte Gruppenzuweisung jeweils die Mittelwerte und Varianzen für die Konstruktwerte berechnet und die Differenzen zwischen den beiden Gruppen gebildet. Der Permutationstest erfasst, ob sich die Mittelwerte und Varianzen der Konstruktwerte über die 5000 Stichproben hinweg signifikant voneinander unterscheiden (d.h. ob die Differenzen der Mittelwerte beziehungsweise der Varianzen signifikant von 0 abweichen). Nur wenn dies sowohl für die Mittelwerte als auch für die Varianzen nicht der Fall ist, sind gleiche Mittelwerte und Varianzen etabliert. Wie Tabelle A8 im Anhang zeigt, konnte die komplette Invarianz des Messmodells nachgewiesen werden, sodass die Verwendung der kompletten Stichprobe (N = 199) zur Schätzung des Akzeptanzmodells zulässig ist. Daher werden die folgenden deskriptiven Analysen und die Schätzung des Strukturgleichungsmodells anhand der kompletten Stichprobe durchgeführt. Eine Ausnahme stellt die Bewertung des Ausmaßes des Vertrauens in verschiedene Entitäten dar, da das Vertrauen in die ConnCar AG nur von der Gruppe von Teilnehmenden bewertet wurde, die einen expliziten Hinweis auf den Anbieter nach dem betrachten des Videos erhalten hatten.

Wie in den vorangegangenen Studien werden zuerst die wahrgenommene Sensibilität der Daten sowie das Vertrauen in den Anbieter deskriptiv analysiert. Die Teilnehmenden nahmen die Fahrzeugidentifikationsnummer (M = 4,51; SD = 1,22), die Herzschlagfrequenz (M = 4,38; SD = 1,36), die Augenbewegungen (M = 4,51; SD = 4,23) sowie Informationen über den aktuellen Standort (M = 4,02; SD = 0,99) als persönlich wahr. Informationen zum aktuellen Zeitpunkt wurden tendenziell persönlich wahrgenommen (M = 3,43; SD = 1,22), während Informationen über den Fahrzeugzustand tendenziell als nicht persönlich betrachtet wurden (M = 2,84; SD = 1,23). Da ebenso wie in den vorangegangenen Studien nicht einzelne Daten, sondern das gesamte Datenpaket zur Nutzung des vernetzten Dienstes zur Steigerung der Sicherheit preisgegeben werden musste, wurde für jeden Teilnehmer ein Datensensibilitätsscore gebildet. Dieser entsprach der Summe aller Sensibilitätsbewertungen bezüglich der preiszugebenden Daten. Der Score konnte zwischen 6 und 30 Punkten variieren. Das Skalenmittel lag bei 18 Punkten. Da der Median des Datensensibilitätsscores in dieser Stichprobe bei 24 Punkten lag, nahmen die Teilnehmenden das preiszugebende Datenpaket als sensibel wahr (Wilcoxon-Test gegen das Skalenmittel von 18 Punkten: Z = 10,62, $p < .001$). Entsprechend der intendierten Manipulation durch die Vorstellung der ConnCar AG als Tochterunternehmen eines deutschen Automobilherstellers, vertrauten die Teilnehmenden (N = 90) der ConnCar AG (M = 2,34; SD = 0,93) tendenziell stärker als einem privaten Anbieter einer Applikation (M = 2,02; SD = 0,89), jedoch etwas weniger als einem Automobilhersteller (M = 2,69; SD = 2,69).

Auch in Studie 3 wurde die Angemessenheit des Messmodells (operationalisiert durch den Fragebogen) mittels eines faktoriellen PLS Validitätstests überprüft, bevor das Strukturgleichungsmodell zur Validierung der Befunde aus Studie 1 als solches geprüft wurde. Die diskriminante Validität des Messmodells wurde anhand des Fornell-Larcker-Kriteriums erfasst (Fornell & Larcker, 1981). Wie Tabelle A9 im Anhang zeigt, konnte nicht für alle Konstrukte eine größere AVE als die Cross-Ladung auf andere latente Konstrukte gefunden werden, sodass das Fornell-Larcker-Kriterium für das in den vorherigen Studien verwendete Messmodell nicht erfüllt wurde. Die AVE der Einstellung gegenüber der Nutzung war geringer als die Cross-Ladung auf die wahrgenommene Nützlichkeit. Ein alternatives Prüfungsverfahren der diskriminanten Validität ist die Inspizierung der Cross-Ladungen. Für alle Items sollte die Ladung für das intendierte Konstrukt höher sein als für alle anderen Konstrukte (Hair et al., 2016). Dieses schwächere Kriterium wurde für das etablierte Messmodell erfüllt (siehe Tabelle A10 im Anhang). Dennoch wurde hier der Anspruch verfolgt, das Fornell-Larcker-Kriterium zu erfüllen.

Tabelle 13. Cross-Ladungen und durchschnittlich erfasste Varianzen (AVEs) für Studie 3 (angepasstes Messmodell)

	ATT	BI	PU	PEOU	IC	PC	PR	TR	SN
ATT	0,837								
BI	0,811	0,947							
PU	0,826	0,806	0,869						
PEOU	0,473	0,417	0,506	0,852					
IC	0,567	0,644	0,507	0,342	0,940				
PC	-0,509	-0,638	-0,501	-0,190	-0,631	0,941			
PR	-0,577	-0,643	-0,542	-0,228	-0,639	0,864	0,906		
TR	0,739	0,670	0,634	0,363	0,626	-0,543	-0,589	0,834	
SN	0,704	0,751	0,626	0,237	0,589	-0,597	-0,573	0,663	0,871

Hinweis: Die AVEs sind auf der Diagonalen abgetragen. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Da in Studie 3, wie auch in den vorangegangenen Studien, für die wahrgenommene Nützlichkeit insgesamt sechs Items abgefragt wurden, bisher jedoch nur vier Items Berücksichtigung fanden, wurde die Skala für die wahrgenommene Nützlichkeit neu bestimmt (siehe Tabelle A7 im Anhang), sodass mit der neuen Skala für die wahrgenommene Nützlichkeit das Fornell-Larcker-Kriterium für alle Konstrukte erfüllt werden konnte (siehe Tabelle 13).

Der PLS Validitätstest für das angepasste Messmodell ergab, dass alle standardisierten Faktorladungen signifikant höher waren als der Schwellwert von 0,70. Darüber hinaus überschritten alle durchschnittlich erfassten Varianzen (AVEs) den Grenzwert von 0,5, während die internen Konsistenz aller latenten Konstrukte (d. h. die Modellfaktoren), erfasst mittels der kompositen Reliabilität ρ und Cronbach's α, größer als 0,7 waren (siehe Tabelle A7 im Anhang). Somit sprechen die Schätzungen der Modellparameter für eine hohe Validität und Reliabilität des angepassten Messmodells inklusive aller seiner Konstrukte. Auch das ursprüngliche, bereits in den vorangegangenen Studien verwendete Messmodell erfüllt die Kriterien für eine angemessene Validität und Reliabilität, wenn für die diskriminante Validität ein schwächeres Kriterium herangezogen wird. Für die weitere Modellberechnung wird jedoch das angepasste Messmodell

verwendet. Auf das ursprüngliche Messmodell in Studie 3 kann dennoch beim Vergleich der Ergebnisse über alle Studien hinweg zurückgegriffen werden.

Nachdem die Angemessenheit des angepassten Messmodells nachgewiesen wurde, kann das hypothetisierte Strukturgleichungsmodell getestet werden. Das aufgestellte Modell konnte $R_{Ad\text{-}justed}$ = 77,8 Prozent der Varianz der Verhaltensintention, 76,8 Prozent der Varianz des wahrgenommenen Privatheitsrisikos sowie 70,7 Prozent der Varianz der Einstellung gegenüber der Nutzung erklären. Um die prädiktive Validität dieser drei latenten Variablen sicherzustellen wurde der Stone-Geisser Q^2 Test angewandt. Alle Q^2-Werte waren signifikant größer als 0 (0,70, 0,60 und 0,51 für die Nutzungsintention, die wahrgenommenen Privatheitsbedenken sowie die Einstellung gegenüber der Nutzung), sodass eine geeignete prädiktive Validität für diese Zielvariablen angenommen werden kann.

Um die Hypothesen zu Forschungsfrage 1 an einem sicherheitsbezogenen vernetzten Mehrwertdienst im Automobil zu validieren, wurde wie in den vorangegangenen Studien eine Bootstrap Analyse auf der Basis von 5000 Stichproben durchgeführt (Hair et al., 2011). Elf von 14 angenommenen Pfadbeziehungen konnten als signifikant nachgewiesen werden. H 1.1, die einen positiven Einfluss der wahrgenommenen Nützlichkeit auf die Einstellung gegenüber der Nutzung vorhersagte, wurde bestätigt (β = 0,68, t = 12,94, $p < .001$). Ebenso konnte ein signifikanter Effekt der wahrgenommenen Nützlichkeit auf die Nutzungsintention nachgewiesen werden (*H 1.2;* β = 0,36, t = 5,78, $p < .01$). Die wahrgenommene Einfachheit der Nutzung hatte einen signifikanten positiven Einfluss auf die wahrgenommene Nützlichkeit (*H 1.3*; β = 0,51, t = 8,11, $p < .001$), jedoch nicht auf die Einstellung gegenüber der Nutzung (*H 1.4;* β = 0,09, t = 1,50, $p > .05$). Im Einklang mit H 1.5 und H 1.6 konnte je ein signifikanter positiver Einfluss der Einstellung gegenüber der Nutzung (*H 1.5;* β = 0,24, t = 2,89, $p < .001$) sowie der sozialen Norm (*H 1.6*; β = 0,28, t = 4,41, $p < .001$) auf die Nutzungsintention nachgewiesen werden. Wie von H 1.7 und H 1.8 vorhergesagt, hatten die Privatheitsbedenken einen signifikanten positiven Einfluss auf das wahrgenommene Privatheitsrisiko (*H 1.7;* β = 0,74, t = 15,47, $p < .001$) sowie einen signifikanten negativen Einfluss auf das Vertrauen in den Anbieter (*H 1.8;* β = -0,55, t = 11,11, $p < .001$). Im Widerspruch zu Hypothese H 1.9 hatte das Vertrauen in den Anbieter keinen signifikanten positiven Einfluss auf die Nutzungsintention (β = -0,01, t = 0,14, $p > .05$). Da jedoch das Vertrauen in den Anbieter einen signifikanten negativen Einfluss auf das wahrgenommenen Privatheitsrisiko hatte, wurde Hypothese H 1.10 bestätigt (β = -0,13, t = 2,69, $p < .01$).

Tabelle 14. Ergebnisse der Prüfung der Hypothesen zu Forschungsfrage 1 am Beispiel eines sicherheitsbezogenen Dienstes.

Hypothese	*Beziehung*	*β*	*t*	*p*	
H 1.1	PU → ATT	0,68	12,94	<.001	H_0 abgelehnt
H 1.2	PU → BI	0,36	5,78	<.001	H_0 abgelehnt
H 1.3	PEOU → PU	0,51	8,11	<.001	H_0 abgelehnt
H 1.4	PEOU → ATT	0,09	1,50	>.05	H_0 nicht abgelehnt
H 1.5	ATT → BI	0,24	2,89	<.01	H_0 abgelehnt
H 1.6	SN → BI	0,28	4,41	<.001	H_0 abgelehnt
H 1.7	PC → PR	0,74	15,47	<.001	H_0 abgelehnt
H 1.8	PC → TR	-0,55	11,11	<.001	H_0 abgelehnt
H 1.9	TR → BI	-0,01	0,14	>.05	H_0 nicht abgelehnt
H 1.10	TR → PR	-0,13	2,69	<.01	H_0 abgelehnt
H 1.11	PR → BI	-0,16	3,76	<.001	H_0 abgelehnt
H 1.12	PR → ATT	-0,19	4,37	<.001	H_0 abgelehnt
H 1.13	IC → PR	-0,10	1,70	>.05	H_0 nicht abgelehnt
H 1.14	IC → PC	-0,63	11,90	<.001	H_0 abgelehnt

Hinweis: Signifikanzniveau ist α = .05. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Der Einfluss des wahrgenommenen Privatheitsrisikos auf die Nutzungsintention (*H 1.11;* β = -0,16, t = 3,76, $p < .001$) war ebenso signifikant wie der Einfluss auf die Einstellung gegenüber der Nutzung (*H 1.12*; β = -0,19, t = 4,37, $p < .001$). Die vermutete Rolle der wahrgenommenen Informationskontrolle konnte hingegen nur teilweise bestätigt werden. Entgegen der Hypothese H 1.13 hatte die wahrgenommenen Informationskontrolle keinen signifikanten negativen Einfluss auf das wahrgenommene Privatheitsrisiko (β = -0,10, t = 1,70, $p > .05$).

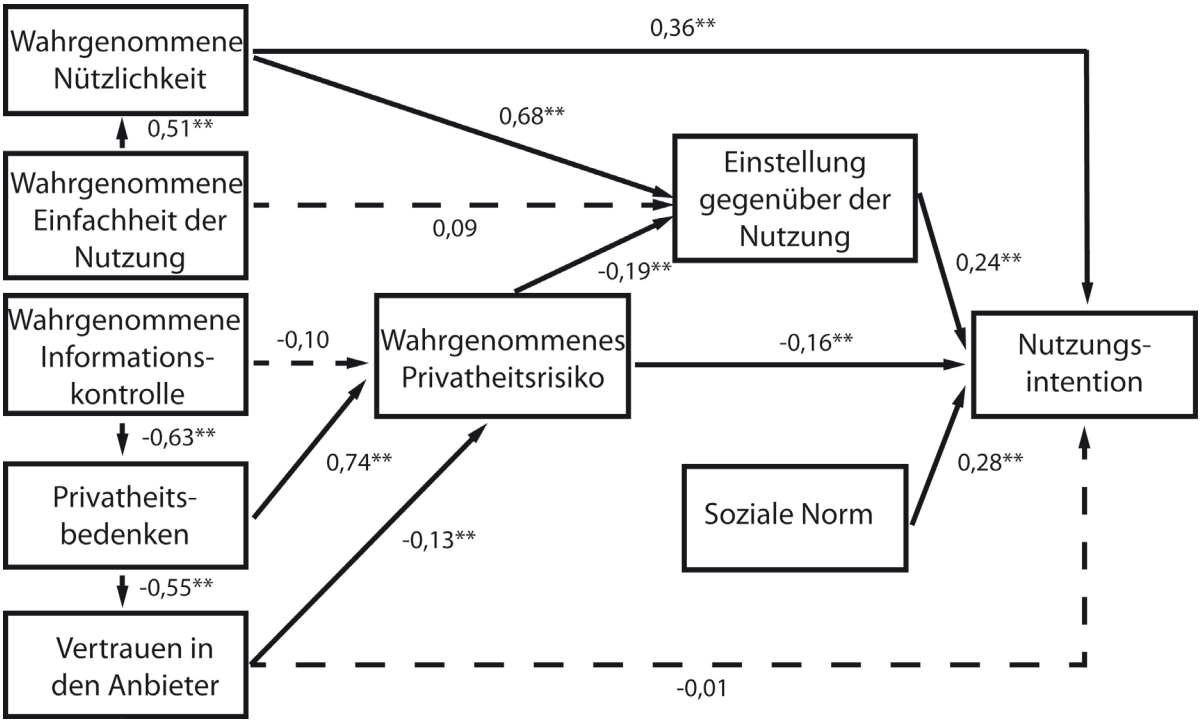


Abbildung 21. Ergebnisse der PLS Strukturgleichungsmodellierung zu den Hypothesen der Forschungsfrage 1 am Beispiel sicherheitsbezogener vernetzter Mehrwertdienste. Dargestellt werden die Pfadkoeffizienten β. Gestrichelte Pfade kennzeichnen nicht signifikante Pfadbeziehungen.

In Einklang mit H 1.14 war jedoch der Einfluss der wahrgenommenen Informationskontrolle auf die Privatheitsbedenken signifikant negativ (β = -0, 63, t = 11,90, p < .001). Tabelle 14 sowie Abbildung 21 fassen die Ergebnisse der PLS Strukturgleichungsmodellierung für vernetzte sicherheitsbezogene Mehrwertdienste zusammen. Die gleiche Analyse wurde nochmals auf Basis der ursprünglichen Skala für die wahrgenommene Nützlichkeit durchgeführt. Die Ergebnisse bestätigen das hier berichtete Strukturgleichungsmodell (siehe Tabelle A11 sowie Abbildung A3 im Anhang).

4.3.3. Diskussion

Sicherheit kann als ein höheres Gut als Komfort und Effizienz betrachtet werden. Im Kontext von vernetzten Diensten im Automobil ziehen Nutzende entsprechend sicherheitsbezogene Dienste komfort- und effizienzbezogenen Diensten vor (Brell, Biermann et al., 2019). In Anlehnung an die Kategorisierung von vernetzten Mehrwertdiensten im Automobil von Walter et al. (2020) ergänzt Studie 3 die vorangegangenen beiden Studien in dem Sinne, dass das in dieser Thesis aufgestellte Akzeptanzmodell an allen funktionalen Kategorien von vernetzten Mehrwertdiensten angewendet wurde. Wie in den vorangegangenen Studien konnte auch am Beispiel sicherheitsbezogener vernetzter Mehrwertdienste im Automobil die grundlegende Modellstruktur im Sinne eines Kosten-Nutzen-Abgleichs repliziert werden. Einerseits beeinflusst die

wahrgenommene Nützlichkeit sowohl die Einstellung gegenüber der Nutzung des sicherheitsbezogenen Dienstes als auch die Intention, diesen zu nutzen. Je einfacher dabei die wahrgenommene Handhabung des Dienstes, desto besser kann der wahrgenommene Nutzen auch erreicht werden. Dem gegenüber stehen privatheitsbezogene Faktoren, die die Bedingungen der Datenpreisgabe und somit die Kosten repräsentieren. Wie bereits in Studie 1, jedoch nicht in Studie 2, stellt das wahrgenommene Privatheitsrisiko den zentralen, privatheitsbezogenen Faktor in dem Akzeptanzmodell am Beispiel sicherheitsbezogener vernetzter Mehrwertdienste im Automobil dar. Das wahrgenommene Privatheitsrisiko wird von den Privatheitsbedenken sowie dem Vertrauen in den Anbieter direkt beeinflusst, während die wahrgenommene Informationskontrolle einen indirekten, von den Privatheitsbedenken vermittelten Einfluss auf das wahrgenommene Privatheitsrisiko hat. Halten Nutzende eines sicherheitsbezogenen vernetzten Mehrwertdienstes im Automobil den Kontrollverlust über die preisgegebenen Daten für wahrscheinlich, haben sie wie auch in andere Kontexten (Featherman et al., 2010; Lee, 2009) eine negativere Einstellung gegenüber der Nutzung des vernetzten Dienstes sowie eine geringere Intention diesen zu nutzen. Im Gegensatz zu komfortbezogenen vernetzten Mehrwertdiensten (Studie 1) findet der Kosten-Nutzen-Abgleich nicht nur in der Einstellung gegenüber der Nutzung des Dienstes, sondern auch in der Nutzungsintention statt. Während die Einstellung gegenüber der Nutzung eine affektive Bewertungskomponente enthält, steht die Nutzungsintention in dem Modell für eine stärker elaborierte Entscheidung für oder gegen die Absicht, den vernetzten Dienst zu nutzen. Vergleicht man die Funktionen von Komfort und Sicherheit, so beinhaltet Komfort eine deutlich stärkere hedonische Komponente. Zieht man die Ergebnisse von Kazakevičiūtė und Banytė (2013) hinzu, die auf Basis einer Literaturanalyse zeigten, dass der wahrgenommene hedonische Wert eines Produkts, neben sozialen und epistemischen, auch durch affektive Bewertungen beeinflusst wird, so scheint es plausible, dass im Fall von komfortbezogenen vernetzten Diensten die Kosten-Nutzen-Abwägung in der affektiv geprägten Einstellung gegenüber der Nutzung des Dienstes mündet. Bei der Wahrnehmung von sicherheitsbezogenen Funktionen bleibt der affektive Aspekt im Kosten-Nutzen-Abgleich vorhanden, verliert jedoch an relativer Relevanz, da der Kosten-Nutzen-Abgleich nun auch die Nutzungsintention direkt miteinbezieht. Dies spiegelt einerseits die erhöhte Relevanz des Nutzens von sicherheitsbezogenen Diensten und andererseits eine höhere Wahrscheinlichkeit von negativen Konsequenzen für die Nutzungsabsicht von sicherheitsbezogenen Diensten wieder, sollte die Wahrscheinlichkeit eines Kontrollverlustes über die preisgegebenen Daten als hoch eingeschätzt werden.

Im Kontext von effizienzbezogenen vernetzten Mehrwertdiensten im Automobil (Studie 2) nahm das Vertrauen in den Anbieter noch eine zentrale Rolle in der Modellstruktur ein, die hier nicht repliziert werden konnte. Wie in der Motivation von Studie 3 bereits aufgeführt, kann die

Nutzungserfahrung als eine besondere Form der Information über den Dienst und seinen Anbieter betrachtet werden. Sollte die prädiktive Rolle des Vertrauens in den Anbieter nicht nur von der Interaktionserfahrung, sondern von Informationen über den Dienstanbieter an sich abhängen, so sollte das Vertrauen in den Anbieter für Teilnehmende, für die die Identität des Dienstanbieters nicht bekannt ist, eine größere prädiktive Rolle spielen. Um diese Nebenhypothese zu testen wurde das Modell nochmals für beide experimentellen Gruppen berechnet. Wie die Tabellen A12 und A13 im Anhang zeigen, unterschieden sich die strukturellen Ergebnisse zwischen beiden experimentellen Gruppen in der Tat lediglich in dem Einfluss des Vertrauens in den Anbieter auf das wahrgenommene Privatheitsrisiko, der nur in der experimentellen Gruppe ohne expliziten Hinweis auf den Datenempfänger signifikant wurde. In Anlehnung an Gefen, Karahanna et al. (2003) wurde in Studie 2 geschlussfolgert, dass der Mangel an tatsächlicher Nutzungserfahrung auch in vernetzten Diensten im Automobil die Rolle des Vertrauens fördert. Studie 3 erweitert diese Sichtweise. Die hiesigen Ergebnisse sprechen dafür, dass nicht die Nutzungserfahrung an sich, sondern das Vorliegen von Informationen über den Anbieter des Dienstes die prädiktive Rolle des Vertrauens in den Anbieter prägt. Allerdings bleibt es unklar, warum in Studie 2 das Vertrauen in den Anbieter einen direkten Einfluss auf die Nutzungsintention hatte, jedoch weder in einer der experimentellen Bedingungen in Studie 3, noch in der Gesamtstichprobe. Diese konnte auf Basis der Ergebnisse der MICOM, die die Vergleichbarkeit und Vereinbarkeit beider Teilstichproben bestätigte, zur Berechnung des Modells herangezogen werden.

Im Gegensatz zu den vorangegangenen Studien wurde hier in Studie 3 eine angepasste Skala für die wahrgenommene Nützlichkeit verwendet, da die ursprüngliche Skala nicht den Ansprüchen des Fornell-Larcker-Kriteriums für die diskriminante Validität gerecht wurde. Zwar erfüllte die ursprüngliche Skala für die wahrgenommene Nützlichkeit den Anspruch, dass jedes beinhaltete Item eine höhere Ladung auf die wahrgenommene Nützlichkeit als auf andere Konstrukte hatte. Da dies jedoch ein schwächeres Kriterium für die diskriminante Validität darstellt und diese in den vorherigen Studien an dem Fornell-Larcker-Kriterium gemessen wurde, wurde hier eine Anpassung der ursprünglichen Skala vorgezogen. Um die Vergleichbarkeit mit den vorherigen Studien dennoch rechtfertigen zu können, wurde die Modellstruktur auch nochmals für das Messmodell mit der ursprünglichen Skala für die wahrgenommene Nützlichkeit berechnet. Unabhängig von der Skalierung der wahrgenommenen Nützlichkeit wurde die identische Modellstruktur erzielt.

5. Allgemeine Diskussion

Die Vernetzung des Automobils ist nicht nur ein Eckpfeiler der Transformation der Automobilbranche (Bosler et al., 2019), sondern gleichzeitig die Grundlage für eine Vielzahl neuer Funktionen, die im Automobil wahrgenommen werden können (Coppola & Morisio, 2016). Mit der Vernetzung hält jedoch auch die Gefahr der Verletzung der informationellen Privatsphäre Einzug in das Automobil (Wachter, 2018). Während Implikationen und Lösungsvorschläge für die informationelle Privatsphäre im Automobil bereits aus juristischer (Roßnagel, 2015), technischer (Makhdoom et al., 2020) und interdisziplinärer Perspektive (Plappert et al., 2017) hervorgebracht wurden, findet die informationelle Privatheit in der Akzeptanzmodellierung im automobilen Kontext trotz existierender Nutzendenbefragungen (z. Bsp. Bloom et al., 2017; Brell, Philipsen et al., 2019; Rohunen & Markkula, 2018) bisher keine Berücksichtigung. Da der Aspekt der Kontrolle über die Datenpreisgabe sowohl in gesetzlichen Vorgaben (GDPR, 2016), Definitionen der Privatheit (Tavani & Moor, 2001; Westin, 1967), interdisziplinären Lösungsansätzen (Plappert et al., 2017) als auch in der Nutzendenperspektive (Brell, Biermann et al., 2019; Svangren et al., 2017) eine zentrale Rolle einnimmt, verfolgte diese Arbeit das Ziel, den Einfluss der Privatheit auf die Akzeptanz und Akzeptierbarkeit von vernetzten Diensten im Automobil modelltheoretisch zu untersuchen (Forschungsfrage 1) und dabei im Besonderen die Rolle der Erfahrung einer tatsächlichen Privatheitskontrolle zu beleuchten (Forschungsfrage 2). Basierend auf der Klassifizierung von vernetzten Mehrwertdiensten im Automobil in komfort-, effizienz- und sicherheitsbezogene Dienste wurden drei Studien durchgeführt, die hier zusammenfassend inhaltlich und methodisch diskutiert werden. Abschließend werden theoretische und praktische Implikationen dieser Arbeit erörtert.

5.1. Diskussion zu Forschungsfrage 1

Die Handlungs- und Akzeptanzmodellierung ist als interdisziplinäres Forschungsfeld schon seit über 50 Jahren etabliert. Besonders mit dem Aufkommen von PCs erfuhr die Akzeptanzforschung einen Aufschwung. Neben vielen anderen Anwendungsfällen und Kontexten ist auch die Mobilität und im Besonderen das Automobil innerhalb der letzten Dekade in den Fokus gerückt. Trotz der oben aufgeführten steigenden Relevanz der Privatheit und deren Kontrolle in vernetzten Automobilen blieben privatheitsbezogene Faktoren in Akzeptanzmodellen im Automobilkontext unberücksichtigt. Gleichzeitig wurde die informationelle Privatheit in verwandten Kontexten wie dem Einsatz ortsbezogener Daten in mobilen Endgeräten intensiv untersucht, sodass der Einfluss privatheitsbezogener Faktoren auf die Nutzung oder Nutzungsintention von datenverarbeitenden Systemen bereits beschrieben ist (Cottrill & Thakuriah, 2015; Wang & Lin, 2016; Xu & Gupta, 2009; Zhao et al., 2012; Zhou, 2012). Auf Basis dieser Studien wurde zur

Beantwortung von Forschungsfrage 1 ein privatheitssensitives Akzeptanzmodell für vernetzte Dienste im Automobil entwickelt, das aufgrund der Modellstruktur als eine Detaillierung des privacy calculus Modells (Dinev & Hart, 2006) verstanden werden kann. Basierend auf dem TAM (Davis, 1986) und der Theory of Planned Behavior (Ajzen, 1985) sagt das Modell einen Abgleich von nutzen- und privatheitsbezogenen Faktoren in der Einstellung gegenüber der Nutzung des Systems sowie der Nutzungsintention des selbigen vorher (siehe Abbildung 10; Kapitel 3). Die das Modell charakterisierende Pfadbeziehungen zwischen den einzelnen Modellfaktoren sind in den Hypothesen 1.1 bis 1.14 beschrieben. In den drei durchgeführten Studien wurde das privatheitssensitive Akzeptanzmodell an je einem komfort-, effizienz- und sicherheitsbezogenen Dienst getestet.

Während die jeweiligen Ergebnisse der Modellevaluationen dem Kapitel 4 entnommen werden können, wird hier zur Beantwortung der Forschungsfrage 1 eine vergleichende Perspektive eingenommen, die alle drei Studien zur Grundlage hat.

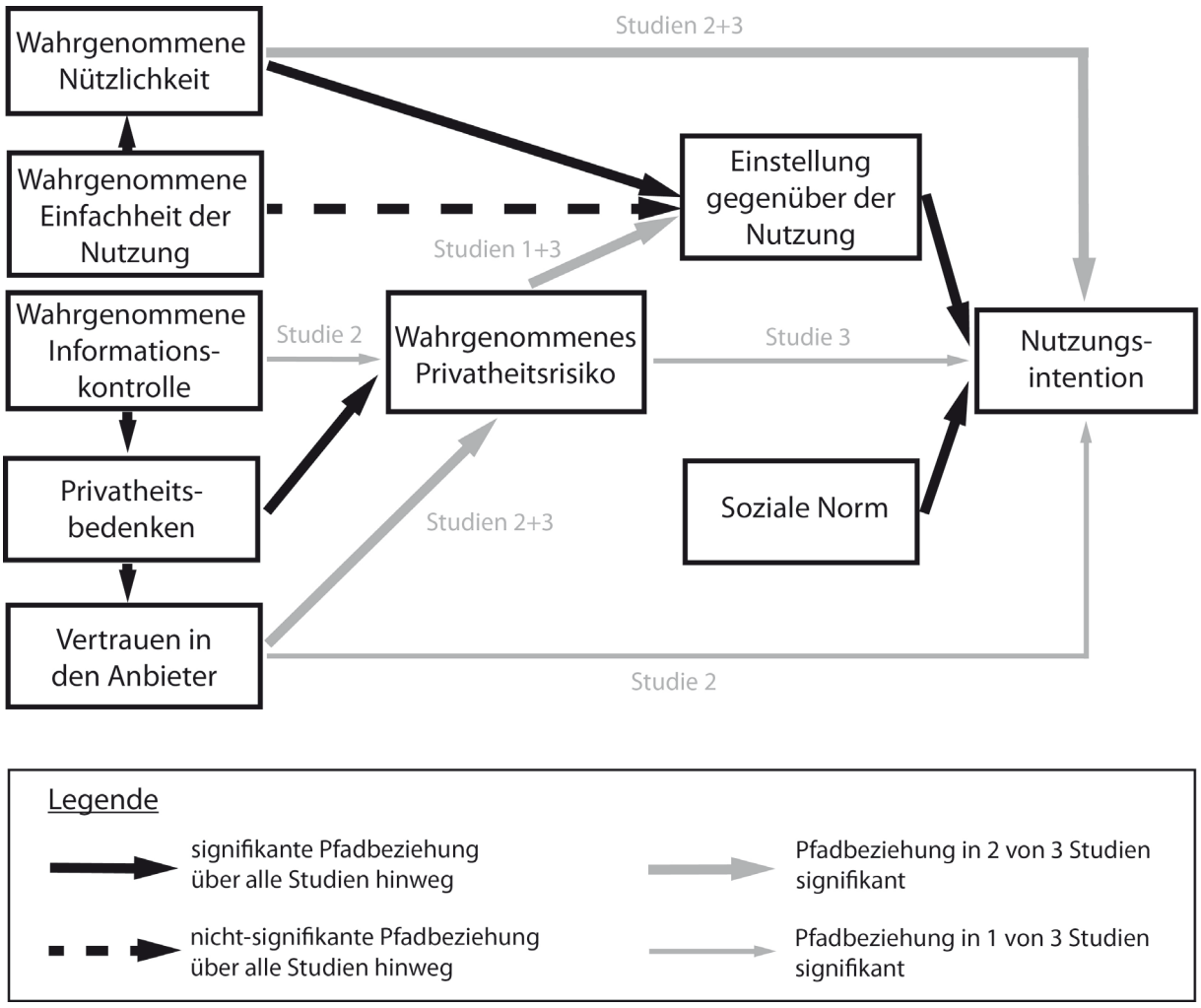


Abbildung 22. Übersicht über alle drei Modellevaluationen hinweg. Schwarze Linien kennzeichnen Pfadbeziehungen, die über alle drei Studien die gleichen Resultate erzielten.

Wie Abbildung 22 zeigt, konnten sieben hypothetisierte Pfadbeziehungen in allen Studien bestätigt werden, während der Einfluss der wahrgenommenen Einfachheit der Nutzung auf die Einstellung gegenüber der Nutzung des Systems in keiner der Studien signifikant wurde. Obwohl unter den sieben, über alle Studien bestätigten Pfadbeziehungen keine Pfadbeziehung zwischen einem privatheitsrelevanten Faktor und der Einstellung gegenüber der Nutzung des Systems oder der Nutzungsintention enthalten ist, hatte in jeder der drei durchgeführten Studien mindestens einer der betrachteten privatheitsrelevanten Faktoren einen Einfluss auf die genannten Zielvariablen. Während dies in den Studien 1 und 3 das wahrgenommene Privatheitsrisiko war, nahm das Vertrauen in den Anbieter in Studie 2 die Rolle des zentralen privatheitsbezogenen Faktors ein. Somit kann die in Forschungsfrage 1 formulierte Frage nach dem Einfluss privatheitsrelevanter Faktoren auf die Nutzung oder Nutzungsintention bejaht werden. Allerdings zeigt Abbildung 22 auch, dass dieser Einfluss nicht über alle Studien hinweg in gleicher Art und Weise erfolgt. Die über alle Studien hinweg bestätigten Einflüsse sowie die Ursachen der teilweise unterschiedlichen Studienergebnisse werden im Folgenden diskutiert.

Über alle Funktionsklassen von vernetzten Diensten im Automobil hinweg konnte bestätigt werden, dass der Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention eines vernetzten Dienstes im Automobil durch die Einstellung gegenüber diesem Dienst moderiert wird. Darüber hinaus beeinflusst die wahrgenommene Einfachheit der Nutzung zwar die wahrgenommene Nützlichkeit des vernetzten Dienstes, hat jedoch keinen direkten Einfluss auf die Einstellung gegenüber dem vernetzten Dienst. Somit gilt für vernetzte Dienste im Automobil, dass die angebotene Funktion, aber nicht der Aufwand, der zu deren Nutzung nötig ist, einer affektiven Bewertung unterliegt, welche die Intention, den vernetzten Dienst zu nutzen, mitbeeinflusst. Darüber hinaus hängt die Bildung der Nutzungsintention von der wahrgenommenen Meinung der nahestehenden Personen bezüglich des Einsatzes des vernetzten Dienstes im Automobil ab. Glaubt eine Person, dass ihr soziales Umfeld den Einsatz eines vernetzten Dienstes unterstützen würde, ist es wahrscheinlicher, dass sie auch die Nutzung dieses Dienstes intendiert. Auch wenn der privatheitsbezogene Modellast keinen über alle Funktionsklassen hinweg konstanten Einfluss auf die Zielvariablen Einstellung zu Nutzung des vernetzten Dienstes oder der Nutzungsintention desselbigen hatte, konnten für vernetzte Dienste im Allgemeinen gültige Einflüsse privatheitsbezogener Faktoren identifiziert werden. Wie bereits in mehreren Kontexten gezeigt werden konnte (Bansal et al., 2010; Zhou, 2012), sind auch Nutzende von vernetzten Diensten im Automobil bezüglich des Umgangs mit den von ihnen preisgegebenen Daten besorgt. Nehmen diese Privatheitsbedenken zu, kann das Vertrauen in den Anbieter darunter leiden, während das wahrgenommene Risiko für die eigene informationelle Privatheit im Zuge der Nutzung des vernetzten Dienstes zunimmt. Dabei trägt das Ausmaß der wahrgenommenen

Möglichkeiten zur Kontrolle der preiszugebenden Daten wie in anderen Anwendungsfällen (Xu et al., 2011; Xu et al., 2013) auch bei vernetzten Diensten im Automobil zu den Privatheitsbedenken bei.

5.1.1. Der direkte Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention

Warum besteht jedoch über die unterschiedlichen Funktionskategorien hinweg kein direkter Einfluss der wahrgenommenen Nützlichkeit auf die Intention, den vernetzten Dienst zu nutzen? Während in Studie 1 dieser Einfluss nicht nachgewiesen werden konnte, gelang dies in Studien 2 und 3 hingegen sehr wohl. Betrachtet man sowohl Unterschiede im Studiendesign als auch der verschiedenen dargebotenen Funktionsklassen über die drei Studien hinweg, leiten sich zwei Erklärungsansätze ab. Einerseits unterscheidet sich Studie 1 von den folgenden Studien im Studiendesign und daraus folgend im Ausmaß der Interaktionserfahrung mit dem vernetzten Dienst im Automobil, die die Teilnehmenden erwerben konnten. Während Studie 1 im Fahrsimulator durchgeführt wurde und den Teilnehmenden eine Interaktionserfahrung ermöglichte, war dies im Zuge der Online-Umfragen der Studien 2 und 3 nicht der Fall. Somit wurde in Studie 1 die Akzeptanz gegenüber einem vernetzten Dienst im Automobil erfasst, während die Studien 2 und 3 die Akzeptierbarkeit mangels Interaktionserfahrung erfassten. Um zu klären ob der direkte Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention im Kontext von vernetzten Diensten im Automobil von dem Vorliegen einer Interaktionserfahrung abhängt, wurden die in Kapitel 2.5 angeführten Studien zur Erfassung der Akzeptanz oder Akzeptierbarkeit von Systemen im automobilen Kontext unter Verwendung des TAM (Davis, 1986) im Hinblick auf das Maß an gebotener Interaktionserfahrung sowie dem direkten Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention betrachtet. Wie Tabelle 15 zeigt, variiert die Signifikanz des Einflusses der wahrgenommenen Nützlichkeit auf die Nutzungsintention nicht in Abhängigkeit von dem Vorhandensein einer Interaktionserfahrung. Sowohl Buckley et al. (2018) als auch Moták et al. (2017) boten ihren Teilnehmenden die Möglichkeit Interaktionserfahrung mit dem jeweiligen System zu erwerben, beobachteten dennoch einen signifikanten Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention. Umgekehrt mangelte es den Teilnehmenden von Chen und Chen (2009) und Sonneberg et al. (2019) an Interaktionserfahrung. Dennoch konnte kein signifikanter Zusammenhang zwischen der wahrgenommenen Nützlichkeit und der Nutzungsintention beschrieben werden.

Tabelle 15. Vergleichende Übersicht über bestehende Akzeptanzstudien im automobilen Kontext auf der Basis des Technology Acceptance Models nach Davis (1986).

Kontext	**Studie**	**Studiendesign**	**Interaktion**	**PU → BI**
Automatisierung	Buckley et al. (2018)	Simulator	ja	signifikant
	Hegner et al. (2019)	Online-Fragebogen	nein	signifikant
	Moták et al. (2017)	Fragebogen plus Feldstudie	ja	signifikant
	Payre et al. (2014)	Online-Fragebogen	nein	signifikant
Elektromobilität	Fazel (2014)	Online-Fragebogen	nein	signifikant
	Wu et al. (2019)	Online-Fragebogen	nein	signifikant
FAS	Ghazizadeh, Peng et al. (2012)	Online-Fragebogen	nein	signifikant
	Park et al. (2015)	Online-Fragebogen	nein	signifikant
Vernetztes Fahren	Chen und Chen (2009)	Online-Fragebogen	nein	nicht signifikant
	Yoon und Cho (2016)	Online-Fragebogen	nein	signifikant
Car Sharing	Simon et al. (2013)	Online-Fragebogen	nein	signifikant
	Sonneberg et al. (2019)	Online-Fragebogen	nein	nicht signifikant

Daher scheint das Vorliegen einer Interaktionserfahrung als erklärender Faktor für Variationen in der Signifikanz des direkten Einflusses der wahrgenommenen Nützlichkeit auf die Nutzungsintention im Kontext vernetzter Dienste im Automobil ungeeignet zu sein. Hingegen unterstützt der Blick auf die bestehenden Studien im automobilen Kontext unter Verwendung des TAM (siehe Tabelle 15) den alternativen Erklärungsansatz, der den Einfluss der dargebotenen Funktion zur Grundlage hat.

Vergleicht man die Studien im Hinblick des Vorliegens eines signifikanten direkten Einflusses der wahrgenommenen Nützlichkeit auf die Nutzungsintention mit den jeweiligen inhaltlichen Studienkontexten, zeigt sich, dass unabhängig von der Interaktionserfahrung alle Studien in den Kontexten Automatisierung, Elektromobilität und FAS einen signifikanten Einfluss berichteten, während Variationen in der Signifikanz dieses Einflusses nur im Kontext des vernetzten

Fahrens sowie des Car Sharings berichtet wurden. Daher legt dieser Vergleich nahe, dass nicht die Interaktionserfahrung, sondern der dargebotene Kontext die Relevanz der wahrgenommenen Nützlichkeit auf die Nutzungsintention beeinflusst. Über die verschiedenen Kontexte variieren auch die Funktionen, die die unterschiedlichen Systeme den Nutzenden anbieten. Funktionale Kontexte, in denen primär sicherheitsrelevante (Automatisierung, FAS) oder effizienzbezogene Funktionen (Elektromobilität) dargeboten werden, sind mit einem direkten Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention assoziiert. Car Sharing und vernetztes Fahren hingegen bedienen neben sicherheits- oder effizienzbezogenen verstärkt auch komfortbezogene Funktionen als die oben genannten Kontexte (vergleiche Walter et al. (2020) für vernetzte Dienste im Automobil). Darüber hinaus beschrieben die beiden in Tabelle 15 aufgeführten Studien im Kontext des vernetzten Fahrens vernetzte Dienste sehr allgemein, indem sie die Vorteile vernetzter Dienste von komfortbezogenen bis hin zu sicherheitsbezogenen Funktionen beschreiben (Yoon & Cho, 2016), oder telematische Dienste untersuchten ohne jedoch in der Veröffentlichung zu konkretisieren, wie diese den Teilnehmenden erklärt und dargeboten wurden (Chen & Chen, 2009). Daher kann der Mangel an einem Bezug zu einem konkreten, greifbaren vernetzten Dienst zu der unklaren Befundlage im Kontext vernetzter Dienste geführt haben (je ein Befund zu einem signifikanten vs. nicht signifikanten Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention; siehe Tabelle 15). Somit legt diese vergleichende Betrachtung zwar nicht nahe, dass ein signifikanter Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention ausschließlich in primär sicherheits- und komfortbezogenen Funktionskontexten möglich ist, während ein stärkerer Komfortbezug einen nicht signifikanten Einfluss bedingt. Jedoch lässt sich schlussfolgern, dass ein direkter Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention bei Systemen, die einen hohen Sicherheits- oder Effizienzbezug haben, wahrscheinlicher ist, als dies der Fall für komfortbezogene Systeme ist. Dies kann auch auf diese Arbeit übertragen werden, sodass die Unterschiede zwischen den Studien im Hinblick auf den direkten Einfluss der wahrgenommenen Nützlichkeit auf die Nutzungsintention nicht durch das Studiendesign, sondern durch die dargebotenen Funktionen erklärt werden kann.

5.1.2. Die Rollen des Vertrauens in den Anbieter sowie des wahrgenommenen Privatheitsrisikos

Ein weiterer, zentraler Unterschied zwischen den Ergebnissen über die drei Studien hinweg ist der Einfluss der privatheitsbezogenen Faktoren auf die Einstellung gegenüber der Nutzung sowie der Nutzungsintention von vernetzten Mehrwertdiensten im Automobil. Während in Studie 1 das wahrgenommene Privatheitsrisiko nur einen Einfluss auf die Einstellung gegenüber der Nutzung hatte, war das wahrgenommene Privatheitsrisiko in Studie 3 hingegen der zentrale

privatheitsbezogene Faktor mit Einfluss sowohl auf die Einstellung gegenüber der Nutzung als auch der Nutzungsintention von vernetzten Mehrwertdiensten im Automobil. Gleichfalls variierte auch die Rolle des Vertrauens in den Anbieter über die Studien hinweg. Während das Vertrauen in den Anbieter in Studie 1 keine prädiktive Rolle spielte, war es in Studie 2 der zentrale privatheitsbezogene Faktor und beeinflusste in Studie 3 das wahrgenommene Privatheitsrisiko. Um den variierenden Einfluss unterschiedlicher privatheitsbezogener Faktoren zu erklären wird hier ein mehrschichtiger Erklärungsansatz bemüht, der auf dem Einfluss der Nutzungserfahrung auf das Vertrauen nach Gefen, Karahanna et al. (2003) aufbaut sowie die Sensibilität der preiszugebenden Daten berücksichtigt.

Gefen und Kollegen (2003) sagen voraus, dass die Relevanz des Vertrauens in den Anbieter bei Vorliegen einer vorherigen Nutzungserfahrung abnimmt. Entsprechend hatte das Vertrauen in den Anbieter in Studie 1 keinen signifikanten Einfluss auf die Intention den vernetzten Mehrwertdienst zu nutzen, während das Vertrauen in den Anbieter in den folgenden Studien 2 und 3 jeweils mindestens das wahrgenommene Privatheitsrisiko vorhersagte. Doch ist es tatsächlich die Nutzungserfahrung per se, die den Einfluss des Vertrauens in den Anbieter moduliert? Studie 3 legt mit der Manipulation der Verfügbarkeit von Informationen über den datenempfangenden Dienstanbieter nahe, dass nicht die Nutzungserfahrung an sich entscheidend sein könnte, sondern vielmehr die Güte der Informationen über den Anbieter. Im Sinne dieser Betrachtungsweise stellt die Nutzungserfahrung dabei nur eine besonders vertrauensvolle, da selbst angeeignete Art einer Information dar, während beim Mangel an Informationen über den Anbieter die Güte der Informationen niedrig ist, da schlicht keine Informationen vorliegen. Die in den Studien 1 bis 3 beobachtete Abnahme des Einflusses des Vertrauens in den Anbieter von Situationen, in denen der datenempfangende Anbieter ungekannt ist (Manipulation Studie 3) bis zu Situationen, in denen Nutzungserfahrung erworben werden konnte (Studie 1), kann daher mit dem Ausmaß der Güte der Informationen über Anbieter erklärt werden. Liegen (schriftliche) Informationen über den Anbieter vor, die jedoch nicht der Verlässlichkeit einer eigenen Nutzungserfahrung entsprechen, sollte der Einfluss des Vertrauens in den Anbieter zwischen diesen Polen liegen. Die variierenden Ergebnisse der Studien 2 und 3 legen nahe, dass das Vertrauen in den Anbieter unter diesen Bedingungen in der Tat einen Einfluss haben kann (Studie 2), dieser jedoch situationsabhängig zu sein scheint beziehungsweise noch durch weitere Faktoren beeinflusst wird (Studie 3). Abbildung 23 stellt die entsprechend vorhergesagten und über die drei Studien hinweg beobachteten Variationen des Einflusses des Vertrauens in den Anbieter dar.

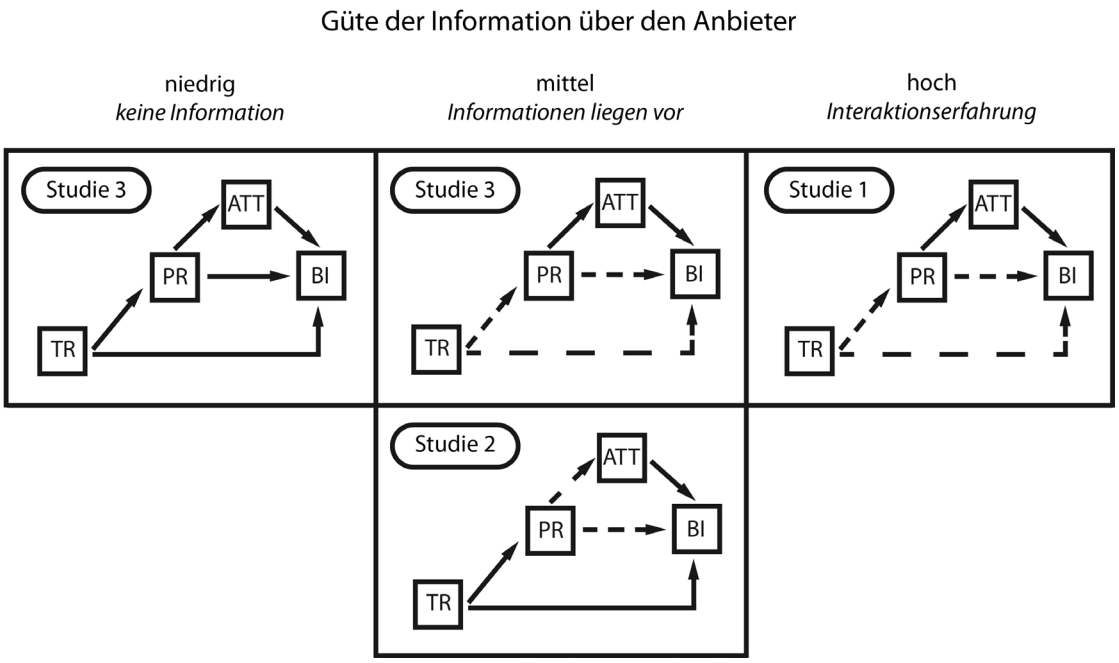


Abbildung 23. Variation des Einflusses des Vertrauens in den Anbieter mit der Güte der Informationen über den Anbieter. Je geringer die Güte der Informationen über den Anbieter, desto höher ist der Einfluss des Vertrauens in den Anbieter. TR = Vertrauen in den Anbieter; PR = Wahrgenommenes Privatheitsrisiko; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Neben dem Vertrauen in den Anbieter scheint auch die Sensibilität der preiszugebenden Daten die Rolle der privatheitsbezogenen Faktoren zu beeinflussen. Frye und Dornisch (2010) fanden bei einem Vergleich der Datenpreisgabe unterschiedlich sensibler Inhalte mittels unterschiedlicher Kommunikationsmedien, dass die Sensibilität des preiszugebenden Inhalts den wahrgenommenen Komfort bei der Datenpreisgabe beeinflusst. Je sensibler ein Inhalt war, desto unwohler fühlten sich die Teilnehmenden bei der Vorstellung, diese Informationen preiszugeben. In dem hiesigen Modell wird zwar das wahrgenommene Komfortempfinden angesichts der Datenpreisgabe nicht direkt erfasst und fungiert ebenfalls nicht wie in Frye und Dornisch (2010) als abhängige Variable. Eine Vielzahl von Studien legt jedoch nahe, dass die wahrgenommene Datensensibilität einen direkten positiven Einfluss auf die Privatheitsbedenken hat (Bansal et al., 2010; Gu et al., 2017; Malhotra et al., 2004b; Milne et al., 2017; Yang & Wang, 2009). Im Einklang mit der bisherigen Literatur verstärkten die Privatheitsbedenken wiederum über alle Studien in der hiesigen Arbeit hinweg das wahrgenommene Privatheitsrisiko. Wird im Zuge der Nutzung eines vernetzten Dienstes im Automobil die Preisgabe von sensiblen Daten erfordert, sollte demnach die prädiktive Rolle des wahrgenommenen Privatheitsrisikos zunehmen (siehe Abbildung 24). Vergleicht man die preiszugebenden Daten über die drei Studien mit der jeweiligen Rolle des wahrgenommenen Privatheitsrisikos (siehe Tabelle 16), so fällt in der Tat ein

Zusammenhang zwischen der Sensibilität des preiszugebenden Datenpakets mit der prädiktiven Rolle des wahrgenommenen Privatheitsrisikos auf.

Dieser lässt sich für den Einfluss des wahrgenommenen Privatheitsrisikos auf die Einstellung gegenüber der Nutzung stabil nachweisen (Studie 1 und 3), während die Auswirkungen auf den direkten Einfluss des wahrgenommenen Privatheitsrisikos auf die Nutzungsintention weniger klar erscheint (signifikanter Einfluss in Studie 3, aber nicht in Studie 1).

Die Datensensibilität wurde in einem digitalen Expertenworkshop mit zwei aktuellen Mitarbeitenden und einer ehemaligen Mitarbeiterin des Instituts für Arbeitswissenschaft durchgeführt, die alle im Zuge ihrer Projekttätigkeiten mit der Bereitschaft zur Datenpreisgabe in datenintensiven Kontexten konfrontiert waren. Hierzu wurde der Prototyp des Parkdienstes (Studie 1) beziehungsweise die animierten Videos (Studien 2 und 3) vorgestellt und die preiszugebenden Datenpakete im Kontext des jeweiligen vernetzten Dienstes im Automobil bezüglich ihrer Sensibilität individuell bewertet und in eine Rangordnung gebracht. Das Datenpaket zur Nutzung des sicherheitsbezogenen Dienstes wurde von zwei Teilnehmenden als am sensibelsten eingeschätzt, gefolgt von dem komfortbezogenen Dienst. Das Datenpaket des effizienzbezogenen Dienstes wurde als am wenigsten sensibel betrachtet. Eine Teilnehmende bewertete das preiszugebende Datenpaket des komfortbezogenen Dienstes als am sensibelsten, gefolgt vom sicherheitsbezogenen und dem effizienzbezogenen Dienst.

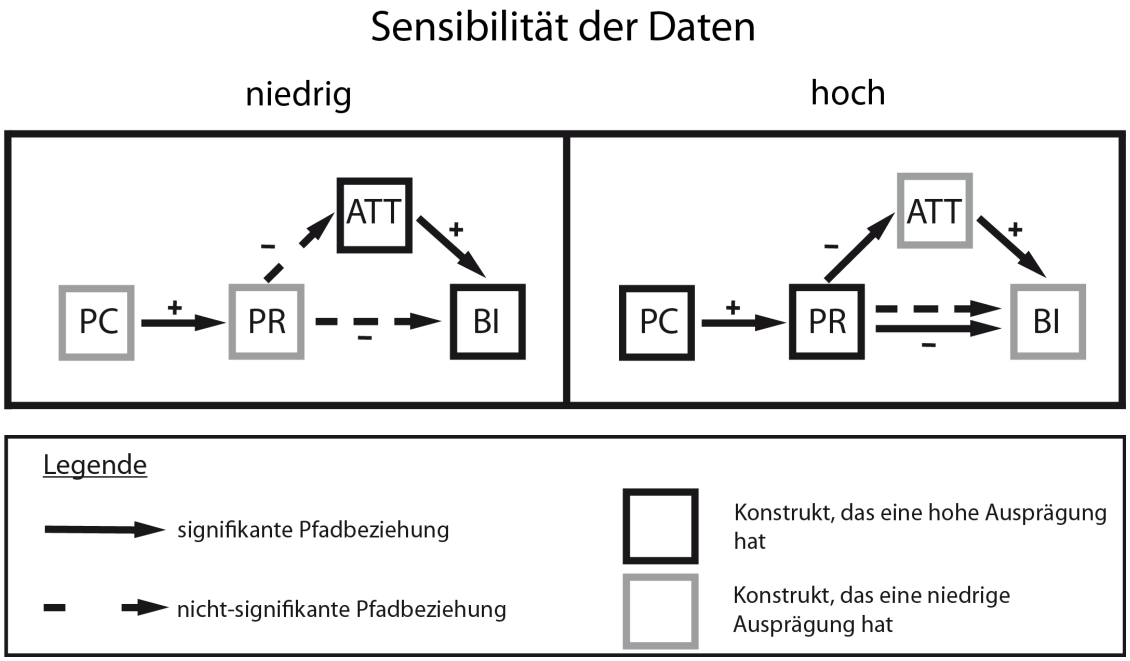


Abbildung 24. Einfluss der Sensibilität der preiszugebenden Daten auf die Rolle des Vertrauens in den Anbieter sowie des wahrgenommenen Privatheitsrisikos. TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Tabelle 16. Gegenüberstellung der preiszugebenden Daten für alle drei Studien inklusive des Rankings der jeweiligen Datenpakete bezüglich der Sensibilität mit der jeweiligen prädiktiven Rolle des wahrgenommenen Privatheitsrisikos (PR) sowie den jeweiligen Signifikanzen der Pfadbeziehungen ausgehend von PR.

Daten	**Studie 1: Komfort**	**Studie 2: Effizienz**	**Studie 3: Sicherheit**
Augenbewegungen			✓
Fahrverhalten	✓	✓	
VIN			✓
Fahrzeugzustand			✓
Herzschlagfrequenz			✓
Identität	✓		
Kalendereinträge	✓		
Routeninformationen		✓	
Standort	✓	✓	✓
Uhrzeit	✓		✓
Sensibilitäts-Ranking (Experten-Workshop)	2	3	1
PR → ATT	signifikant	nicht signifikant	signifikant
PR → BI	nicht signifikant	nicht signifikant	signifikant

Hinweis: PR = Wahrgenommenes Privatheitsrisiko; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention. VIN = Fahrzeugidentifikationsnummer (englisch: vehicle identification number).

Abschließend wurden die Teilnehmenden gebeten in einer Diskussion eine gemeinsame Reihenfolge zu erarbeiten. Die Teilnehmenden verständigten sich auf den sicherheitsbezogenen Dienst als den Dienst mit dem sensibelsten Datenpaket, während der effizienzbezogene Dienst die Preisgabe des am wenigsten sensiblen Datenpakets erforderte (siehe Tabelle 16).

Damit kann aus dem Vorliegen einer vorherigen Interaktionserfahrung sowie der durch Experten gestützte Sensibilität des preiszugebenden Datenpakets der folgende Erklärungsansatz für die hiesigen Befunde bezüglich der unterschiedlichen Rollen des Vertrauens in den Anbieter sowie des wahrgenommenen Privatheitsrisikos verwendet werden:

Während die Rolle der wahrgenommenen Privatheitsrisikos mit der Sensibilität der preiszugebenden Daten variiert, moduliert die Güte der Informationen über den datenempfangenden Anbieter die prädiktive Rolle des Vertrauens in den Anbieter. Liegt eine vorherige Interaktionserfahrung als besonders hohe Ausprägung der Güte der Informationen über den Anbieter vor, so wird die prädiktive Rolle des Vertrauens in den Anbieter reduziert (Gefen, Karahanna et al., 2003). Darüber hinaus beeinflusst die Sensibilität der preiszugebenden Datenpakete, mediiert über die Privatheitsbedenken (Gu et al., 2017), die Rolle des wahrgenommenen Privatheitsrisikos. Je sensibler das preiszugebende Datenpaket ist, desto mehr Einfluss hat das wahrgenommene Privatheitsrisiko auf die Vorhersage der Nutzungsintention sowie der Einstellung gegenüber der Nutzung vernetzter Dienste im Automobil. Betrachtet man die Güte der Informationen über den Anbieter mit den drei Ausprägungen *niedrig, mittel* und *hoch* sowie die Sensibilität der preiszugebenden Daten mit den zwei Stufen *niedrig* und *hoch*, so ergeben sich sechs Szenarien. Die aus dem obigen Erklärungsansatz abgeleiteten Vorhersagen für die jeweiligen Szenarien sind in Abbildung 25 dargestellt. Mit zunehmender Güte der Information über den Anbieter nimmt die prädiktive Rolle des Vertrauens in den Anbieter (von Spalte 1 bis 3) ab, während die Vorhersagekraft des wahrgenommenen Privatheitsrisikos mit der Sensibilität der preiszugebenden Daten abnimmt (von Zeile 1 zu 2).

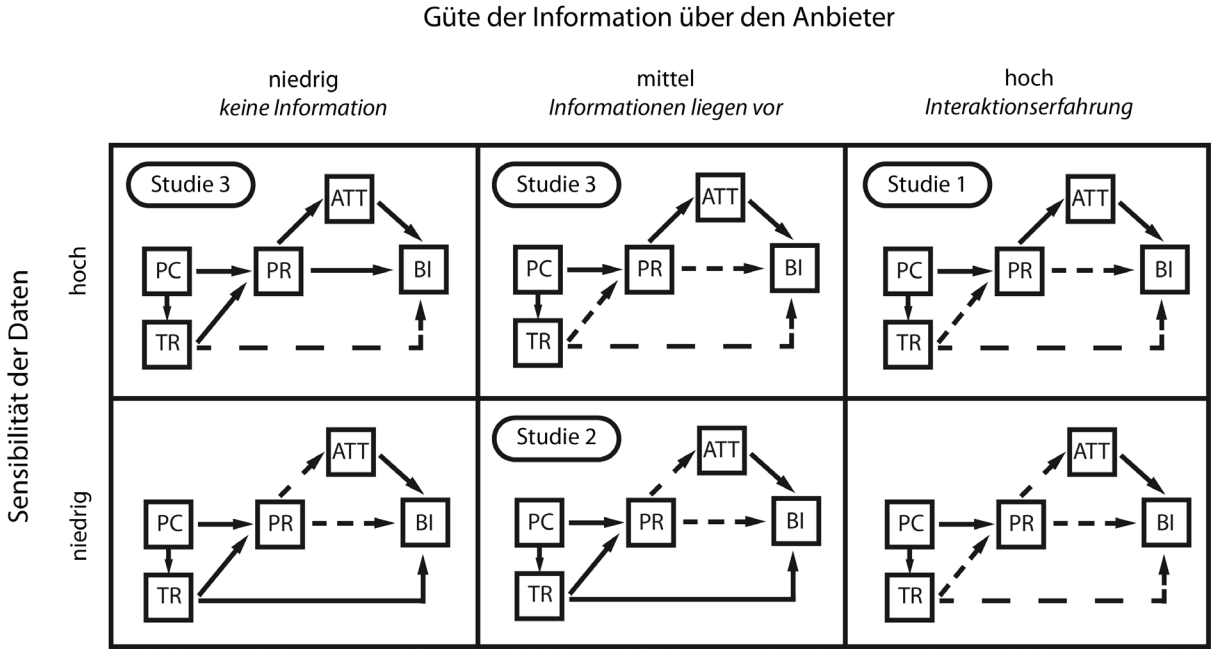


Abbildung 25. Vorhersage der Rolle der privatheitsbezogenen Faktoren in Abhängigkeit von der Güte der Informationen über den datenempfangenden Anbieter sowie der Sensibilität der preiszugebenden Daten. Szenarien, die in den Studien 1-3 abgedeckt wurden, sind entsprechend markiert. TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

In den hier durchgeführten Studien konnten vier von sechs Szenarien abgebildet werden. Dabei scheinen die Ergebnisse von Studie 3, die dem Szenario mit einer niedrigen Güte der Information über den Anbieter sowie einer hohen Sensibilität der preiszugebenden Daten entsprechen (Abbildung 25 oben links), den Vorhersagen zu widersprechen. Was auf den ersten Blick ein Widerspruch zu sein scheint, lässt sich jedoch unter Einbezug der Betrachtung der Datensensibilität erklären. Da unter der Bedingung einer hohen Sensibilität der preiszugebenden Daten das wahrgenommene Privatheitsrisiko eine hohe Vorhersagekraft hat, wird der postulierte direkte Einfluss des Vertrauens in den Anbieter auf die Nutzungsintention vollständig über das wahrgenommene Privatheitsrisiko mediiert. Entsprechend ist auch das in Studie 3 beschriebene Szenario das einzige, in dem das wahrgenommene Privatheitsrisiko einen signifikanten direkten Einfluss auf die Nutzungsintention hat. Somit hat das Vertrauen in den Anbieter auch unter den Bedingungen einer hohen Datensensibilität und dem Mangel an Informationen über den datenempfangenden Anbieter einen ausgeprägten Einfluss auf die Nutzungsintention. Dieser wird jedoch durch das wahrgenommene Privatheitsrisiko mediiert.

Die Szenarien mit einer niedrigen Datensensibilität und einer niedrigen (Abbildung 25 unten links) oder hohen Güte der Informationen über den datenempfangenden Anbieter (Abbildung 25 unten rechts) wurden in dieser Arbeit nicht abgedeckt. Der hier bemühte Erklärungsansatz erlaubt es jedoch für zukünftige Studien konkrete Vorhersagen abzuleiten. So sollten zum Beispiel unter der Bedingung einer niedrigen Datensensibilität sowie dem Vorliegen von Nutzungserfahrung mit dem vernetzten Dienst die privatheitsrelevanten Faktoren keinen signifikanten Einfluss auf die Intention, einen solchen Dienst zu nutzen, haben.

5.1.3. Die Beziehung zwischen der wahrgenommenen Informationskontrolle und dem wahrgenommenen Privatheitsrisiko

Die wahrgenommene Informationskontrolle beeinflusste in allen Studien das wahrgenommene Privatheitsrisiko indirekt über die Privatheitsbedenken. Lediglich in Studie 2 bestand ein zusätzlicher direkter Einfluss der wahrgenommenen Informationskontrolle auf das wahrgenommene Privatheitsrisiko. Betrachtet man sich die vorherigen Studien, die einen direkten Einfluss der wahrgenommenen Informationskontrolle auf das wahrgenommene Privatheitsrisiko fanden (Hajli & Lin, 2016; Krasnova et al., 2010), so teilen diese Studien die Eigenschaften, dass sie die Privatheitsbedenken zwar in der Hypothesenbildung betrachten (Hajli & Lin, 2016), jedoch nicht in ihr Modell integrieren. Dabei zeigten bereits Malhotra et al. (2004a) den engen Bezug zwischen Kontrolle und Privatheitsbedenken auf. Auch die Ergebnisse aller drei Studien hier bestätigen den Einfluss der wahrgenommenen Informationskontrolle auf die Privatheitsbeden-

ken, die wiederum das wahrgenommene Privatheitsrisiko verstärken. Während das methodische Vorgehen insbesondere zwischen den Studien 2 und 3 nahezu identisch ist, unterscheiden sich beide Studien sowohl in den angebotenen Funktionen als auch in den preiszugebenden Daten. Wie bereits im Zuge der Diskussion der unterschiedlichen Rolle des wahrgenommenen Privatheitsrisikos über alle drei Studien hinweg, könnte die Datensensibilität auch hier eine mögliche Erklärung liefern. Mit den Studien 1 und 3 wird das wahrgenommene Privatheitsrisiko ausschließlich über einen durch die Privatheitsbedenken mediierten Einfluss von der wahrgenommenen Informationskontrolle beeinflusst, während in Studie 2 zusätzlich ein direkter Effekt gefunden wurde. Dieses Bild passt exakt zu den in dem obigen Expertenworkshop zur Bewertung der objektiven Datensensibilität gefundenen Sensibilitätsunterschieden zwischen den einzelnen Studien. Wird die Preisgabe sensibler Datenpakte erforderlich, wird der Einfluss der Informationskontrolle komplett durch die Privatheitsbedenken mediiert, während bei einer geringeren Sensibilität der Datenpakete lediglich eine teilweise Mediation zu beobachten ist. Da sich letztere dadurch auszeichnet, das neben dem Mediationseffekt auch der direkte Effekt zwischen der unabhängigen (hier: wahrgenommene Informationskontrolle) und der abhängigen Variable (hier: wahrgenommenes Privatheitsrisiko) bestehen bleibt (MacKinnon et al., 2007), scheint die Sensibilität des preiszugebenden Datenpakets das Ausmaß der Mediation über die Privatheitsbedenken zu beeinflussen.

5.2. Diskussion zu Forschungsfrage 2

Die Forderung nach tatsächlicher Kontrolle über die preisgegebenen Daten ist ein wiederkehrendes Thema sowohl in Nutzendenbefragungen (Brell, Biermann et al., 2019; Walter & Abendroth, 2018) sowie in juristischen Beiträgen (Akalu, 2018; Wachter, 2018). Die Auswirkung der Bereitstellung einer solchen Kontrollmöglichkeit auf die Akzeptierbarkeit und Akzeptanz wurden kontextübergreifend selten und im automobilen Kontext entsprechend des Kenntnisstands des Autors noch gar nicht untersucht. Daher wurde in Studie 1 durch den Vergleich der Nutzung eines vernetzten Parkdienstes ohne versus mit Kontrollmöglichkeit über die Datenpreisgabe untersucht, welchen Einfluss eine tatsächliche Informationskontrolle auf die Akzeptanz des vernetzten Dienstes im Automobil hat. Wie bereits in Kapitel 4.1.3 diskutiert, führte die tatsächliche Informationskontrolle im Einklang mit der Theory of Planned Behavior (Ajzen, 1985) zu einer erhöhten wahrgenommenen Informationskontrolle. Ebenso wurden die Privatheitsbedenken sowie das wahrgenommenen Privatheitsrisiko gesenkt, während die Einstellung gegenüber der Nutzung des vernetzten Dienstes positiver wurde. Allerdings konnte neben dem Vertrauen in den Anbieter auch bei der Nutzungsintention keine signifikante Erhöhung durch das Vorliegen einer tatsächlichen Informationskontrolle beobachtet werden. Da die Nutzungsintention generell als Stellvertretung für die Akzeptierbarkeit beziehungsweise Akzeptanz dient, muss

Forschungsfrage 2 verneint werden. Dennoch zeigen die Ergebnisse aus Studie 1, dass Forderungen nach einer tatsächlichen Informationskontrolle nicht nur Lippenbekenntnisse sind. Mit der Ausnahme des Vertrauens in den Anbieter konnten privatheitsbezogene Bedenken und wahrgenommene Risiken gesenkt werden, sodass die Einstellung gegenüber der Nutzung des vernetzten Dienstes signifikant positiver ausfiel als ohne eine solche Kontrollmöglichkeit. Auch wenn nicht signifikant, zeigte sich eine deutliche Tendenz zu einer auch statistisch bedeutsamen Erhöhung der Nutzungsintention durch die Einführung der tatsächlichen Informationskontrolle.

5.2.1. Datensensibilität als möglicher Moderator des Einflusses der tatsächlichen Informationskontrolle

Die Nicht-Signifikanz des Effekts der tatsächlichen Informationskontrolle auf die Nutzungsintention kann durch den spezifischen Untersuchungskontext in Studie 1 bedingt sein. Der bereits im Zuge der Diskussion von Forschungsfrage 1 betrachtete Einfluss der Datensensibilität führte vermutlich dazu, dass das wahrgenommene Privatheitsrisiko keinen direkten Einfluss auf die Nutzungsintention hatte. Wie die obige Diskussion zeigte, scheint ein direkter Einfluss des wahrgenommenen Privatheitsrisikos auf die Nutzungsintention nur gegeben zu sein, wenn besonders sensible Datenpakte zur Diskussion stehen. Entsprechend lässt sich aus diesem Erklärungsansatz die Hypothese ableiten, dass bei Vorliegen von sensibleren Datenpaketen die tatsächliche Informationskontrolle einen signifikanten Einfluss auch auf die Nutzungsintention haben sollte. Während die Sensibilität des Datenpakets des vernetzten Parkdienstes nicht hoch genug war, könnte eine Replikation der Studie 1 am Beispiel des vernetzten sicherheitsbezogenen Dienstes aus Studie 3 auch einen signifikanten Effekt der tatsächlichen Informationskontrolle auf die Nutzungsintention ergeben. Gestärkt wird diese Vermutung durch das Ergebnis der MGA, die keine strukturellen Unterschiede in den Modellen ohne versus mit einer tatsächlichen Informationskontrolle fand. Daher scheint die Übertragbarkeit von Interpretationen auf Basis des Modells ohne tatsächliche Informationskontrolle auf das Modell mit der selbigen gegeben zu sein.

5.2.2. Risiken vermeintlicher Möglichkeiten zur Informationskontrolle

Die Bereitstellung einer Möglichkeit zur Informationskontrolle muss der Wahrung der informationellen Privatsphäre jedoch nicht immer zuträglich sein. Während die hier eingesetzte Datenschutzapplikation PRICON unter Einbezug von informationstechnischen, juristischen und nutzendenseitigen Perspektiven entwickelt (Plappert et al., 2017) und bezüglich seiner Wirksamkeit evaluiert wurde (Walter et al., 2018), zeigen andere Studien die potentielle Gefahr des

Einsatzes nicht ausreichend wirksamer (Brandimarte et al., 2013) oder zu komplexer Kontrollmöglichkeiten auf (Keith et al., 2014). Brandimarte und Kollegen zeigten, dass solche Ansätze, die lediglich die wahrgenommene Informationskontrolle steigern ohne eine tatsächliche Erhöhung der Kontrolle zu bewirken, nicht zwingend zu einem privatheitswahrenden Verhalten führen. Im Einklang mit den Vorhersagen des hier etablierten Akzeptanzmodells für vernetzte Automobile kann die wahrgenommene, aber nicht tatsächlich vorliegende Informationskontrolle zu einer unangemessenen Absenkung der Privatheitsbedenken führen, die den tatsächlichen Privatheitsrisiken nicht gerecht werden (Brandimarte et al., 2013). Unter dem Eindruck der Kontrollmöglichkeit wägen sich Nutzende in der sicheren Position der Kontrollierenden und sind eher bereit Daten preiszugeben. Ein Beispiel hierfür liefern auch Arcand et al. (2007), die zeigten, dass die schiere Präsenz einer Datenschutzerklärung die wahrgenommene Informationskontrolle erhöht. Selbst wenn eine tatsächliche Kontrollmöglichkeit technisch wirksam ist, folgt daraus nicht zwingend, dass die Kontrollmöglichkeit auch zu einer angemesseneren Datenpreisgabe führt. Keith et al. (2014) führten den Begriff der *Privatheitsmüdigkeit* (englisch: *privacy fatigue*) ein und beschreiben damit den Befund, dass zu komplexe Kontrollmöglichkeiten zu einer erhöhten Datenpreisgabe führen. Werden Nutzende mit (sehr) liberalen Standarddatenschutzeinstellungen auf der einen Seite und einer komplexen Möglichkeit zur Informationskontrolle auf der anderen Seite konfrontiert, sind die Nutzenden eher geneigt mehr Daten preiszugeben, selbst wenn die Datenpreisgabe als zu weitreichend wahrgenommen wird. Die Komplexität der Informationskontrolle hält sie nach Keith und Kollegen jedoch von einer datensparsameren Nutzung ab.

5.3. Allgemeine theoretische Diskussion

Diese Arbeit ist geprägt von dem modell-theoretischen Ansatz der Akzeptanzmodellierung. Während die Forschung innerhalb der letzten Jahrzehnte verschiedene Modellierungsansätze für die Erklärung der Nutzung von Technologien oder Handlungen im Allgemeinen hervorgebracht hat, basiert das hier aufgestellte Modell zur Erklärung der Akzeptanz und Akzeptierbarkeit von vernetzten Diensten im Automobil primär auf dem TAM (Davis, 1986) und wird durch Elemente der Theory of Planned Behavior (Ajzen, 1985) ergänzt. Damit werden zwar einerseits die dominanten Modelle innerhalb der Akzeptanzmodellierung herangezogen. Andererseits wird jedoch besonders das TAM für seinen starken kognitiven Fokus und dem Mangel an der ausreichenden Berücksichtigung von affektiven Entscheidungskomponenten kritisiert (Baron et al., 2006; Kulviwat et al., 2007; Read et al., 2011). Fazio (1990) präsentiert mit dem *Motivation and Opportunity as Determinants (MODE) model* einen Ansatz, der berücksichtigt, dass die menschliche Entscheidungsfindung sowohl elaborativ als auch affektiv beziehungsweise spon-

tan erfolgen kann. Damit bietet Fazio (1990) ebenso wie Kulviwat et al. (2007) eine Modellgrundlage, die nicht nur die Rolle des Affekts in der Nutzungsentscheidung berücksichtigt, sondern auch die begrenzte Rationalität, die nach Pelteret und Ophoff (2016) auch auf privatheitsbezogene Entscheidungen zutrifft, abbilden kann. Auch wenn in dieser Arbeit über alle Studien hinweg ein ausgesprochen hoher Anteil der Varianz in der Nutzungsintention erklärt werden konnte, scheint Fazios (1990) MODE Model eine lohnenswerte Basis für zukünftige Studien zu sein, um die Rolle des Affekts sowie den Fakt der begrenzten menschlichen Informationsverarbeitungsressourcen auch im vernetzten Automobil zu berücksichtigen.

Mangels bestehender privatheitsbewusster Akzeptanzmodelle im automobilen Kontext wurden die betrachteten privatheitsbezogenen Faktoren und ihre Beziehungen untereinander aus Studien besonders des Kontexts mobiler Endgeräte abgeleitet. Zwar wurde der Bildschirm zur Einwilligung zur Datenpreisgabe in Studie 1 an das Layout von Android Smartphones angelehnt. Doch trotz dieser graphischen Ähnlichkeiten hat der Nutzungskontext einen substantiellen Einfluss auf die Nutzungsintention von Systemen (Proust, 2012) und, falls gegeben, auch die Datenpreisgabe. Während die Vernetzung bei der Nutzung von mobilen Endgeräten wie dem Smartphone offensichtlicher ist, nehmen Nutzende das Automobil, trotz aller affektiven Beziehungen, primär als Transportmittel wahr (Steg, 2005). Die Vernetzung im Automobil hingegen ist weniger offensichtlich (Federation internationale de l'automobile, 2016; Karaboga et al., 2015). Der Einfluss des Kontexts und im Speziellen der Unterschiede in der Salienz der Vernetzung wird in Dienlin's (2014) *privacy process model* aufgegriffen. Das privacy process model postuliert, dass privatheitsbezogenes Verhalten nicht direkt von der objektiven Privatheitssituation abhängt, sondern vielmehr von der subjektiven Wahrnehmung der selbigen. Falls also die Privatheitsrelevanz im vernetzten Automobil für die Nutzenden weniger offensichtlicher ist, sollten sich Entscheidungen bezüglich der Datenpreisgabe von denen im Kontext des Smartphones unterscheiden. Die hiesigen Ergebnisse sprechen jedoch dafür, dass die Faktorbeziehungen aus dem Smartphonekontext auch auf das vernetzte Automobil übertragbar sind. Allerdings wurde in dieser Arbeit kein direkter Vergleich der Kontexte des vernetzten Automobils und des Smartphones vorgenommen, sodass es eine Aufgabe für zukünftige Studien bleibt den von Dienlin (2014) postulierten potentiellen Einfluss von unterschiedlich salienten Privatheitsrelevanzen in unterschiedlichen Kontexten zu beleuchten. Die Analyse und der Vergleich von mentalen Modellen der jeweils betrachteten Szenarien könnte ein vielversprechender Ansatz sein.

In der Mehrheit der Studien im Kontext der Prädiktion der Nutzung von Systemen werden die Konzepte der Akzeptierbarkeit, Akzeptanz und Adoption nicht unterschieden, obwohl diese Konzepte sehr wohl differenzierbar sind (Nadal et al., 2019). Trotz dieser theoretischen Diffe-

renzierung ist es jedoch bisher unklar, welche Folgen diese Unterscheidung für die Modellierung hat. Gibt es Faktorbeziehungen, die nur bei der Vorhersage der Akzeptierbarkeit, aber nicht der Akzeptanz bestehen? Hier leistet die hiesige Arbeit einen ersten Beitrag, um diese Forschungslücke zu schließen. Im Kontext vernetzter Dienste im Automobil spielt das Vertrauen in den Anbieter nur bei der Prädiktion der Akzeptierbarkeit eine Rolle. Entscheidend ist für den Einbezug des Vertrauens in den Anbieter in die Entscheidungsfindung bezüglich der Nutzungsintention eines vernetzten Systems das Ausmaß an vorhandenen Informationen über den vernetzten Dienst. Wie der Vergleich über die drei Studien in dieser Arbeit zeigt, spielt das Vertrauen in den Anbieter nur eine Rolle, wenn es an Nutzungserfahrung mangelt und somit per Definition die Akzeptierbarkeit eines vernetzten Dienstes im Automobil erfasst wird. Dabei ist die Nutzungserfahrung jedoch nur als ein spezieller Fall an Information zu sehen. Wie die Manipulation der Bekanntheit des Dienstanbieters in Studie 3 zeigt, nimmt die prädiktive Rolle des Vertrauens in den Anbieter zu, je weniger Informationen über die datenempfangende Partei verfügbar sind. Auch wenn weitere Studien diesen Befund erst noch replizieren müssen, legen die hiesigen Ergebnisse im Einklang mit der Prädiktion von Gefen, Karahanna et al. (2003) nahe, dass bei der Erfassung der Akzeptierbarkeit das Vertrauen in den Anbieter eine prädiktive Rolle spielt. Diese nimmt weiter zu, je weniger Informationen über die Nutzung des Systems oder dessen Anbieter vorhanden sind.

5.4. Methodische Diskussion

Das experimentelle Design einer Studie sowie die Auswahl geeigneter Analysemethoden sind die Basis jeder Forschung. Daher sollen hier die angewandten Designs und Methoden reflektiert und kritisch bewertet werden. Ausgehend von einer Makroperspektive werden zuerst die Aspekte diskutiert, die alle drei Studien betreffen, um sich abschließend dem Vorgehen der ersten Studien nochmals gesondert zu widmen.

5.4.1. Allgemeine Methodik

Entsprechend der Tradition der Akzeptanzforschung wurden zur Beantwortung der zentralen Forschungsfragen ein fragebogenbasiertes Vorgehen gewählt. Hierzu wurden zur Bildung des Messmodells Items und Skalen der betrachteten Konstrukte aus der bestehenden Literatur abgeleitet und in einem Fragebogen zusammengeführt. Dabei wurde darauf geachtet, dass jedes Konstrukt durch mindestens drei Items erfasst wird, um eine ausreichende Validität des Messmodells zu gewährleisten (Rigdon et al., 2017). Trotz des hohen Literaturbezugs mussten die ausgewählten Items einer jeden Skala mindestens übersetzt und meist auch an den Kontext des vernetzten Automobils angepasst werden. Entsprechend war eine Überprüfung der Angemessenheit des für den neuen Kontext angepassten Messmodells notwendig (Hair et al., 2016). Dies

erfolgte in der Vorbereitung von Studie 1 im Zuge eines Pretests, der in der Tat auch einige Verbesserungen und Anpassungen nahelegte. Wie die Gütekriterien in Studie 1 zeigen, konnte ein valides und zuverlässiges Messmodell entwickelt werden. Über die unterschiedlichen vernetzten Dienste in den drei Studien hinweg wurde das Messmodell nur marginal angepasst, sodass auf erneute Pretests verzichtet wurde. Während dieses Vorgehen in Studie 2 durch die Gütekriterien bestätigt wurde, konnte das ursprüngliche Messmodell in Studie 3 das Forner-Larcker-Kriterium für die diskriminante Validität nicht erfüllen. Zwar konnte diese für ein ebenfalls anerkanntes, jedoch schwächeres Kriterium in Form der Analyse der Cross-Ladungen (Hair et al., 2016) etabliert werden. Da jedoch in den vorangegangenen Studien das Messmodell an dem Forner-Larcker-Kriterium gemessen wurde, wurde die Skala für die wahrgenommene Nützlichkeit angepasst, sodass ein angepasstes Messmodell die bereits vorher verwendeten Gütekriterien vollständig erfüllte. Durch die minimale Anpassung des Messmodells wurde die Aussage der Skala für die wahrgenommene Nützlichkeit nicht verändert (vergleiche hierzu die beiden Skalen der wahrgenommenen Nützlichkeit in Tabelle A7 im Anhang), aber die Qualität des Messmodells gesteigert.

In allen drei Studien wurden relativ kleine Stichproben für klassische SEM Studien verwendet. In der aktuellen wissenschaftlichen Literatur finden sich Beiträge, die PLS SEM auch für kleine Stichproben geeignet halten (Hair et al., 2011; Wong, 2013), während andere diese Eignung bezweifeln (Goodhue et al., 2012). Um dieser andauernden Debatte zu entgehen wurde hier die kritische minimale Stichprobengröße auf Basis der statistischen *power* entsprechend den Empfehlungen von Cohen (1992) berechnet. Entsprechend gängiger Annahmen (Wong, 2013) wurde für eine statistische Power von 80 Prozent, einem Signifikanzniveau von fünf Prozent, einer erwarteten aufgeklärten Varianz von mindestens $R^2 = 0{,}25$ und einer maximalen Anzahl an Pfadbeziehungen, die auf ein Konstrukt zeigen, von fünf eine Mindeststichprobengröße von $N_{min} = 45$ abgeleitet. Mit den hiesigen Stichprobengrößen von $N > 106$ liegen alle Studien deutlich über dieser geforderten Stichprobengröße. Trotz der nachgewiesenen Eignung der Stichprobengröße erhöhen die dennoch relativ kleinen Stichprobengrößen die Relevanz der adäquaten Abbildung relevanter demographischer Variablen in den jeweiligen Stichproben. Die Erfahrung mit mobilen datenintensiven Kontexten könnte besonders in Studie 1 die wahrgenommene Einfachheit der Nutzung und damit letztendlich auch die Nutzungsintention des vernetzten Dienstes beeinflussen. Um einen Eindruck der Erfahrung mit mobilen datenintensiven Kontexten zu erlangen wurde in allen drei Studien die Smartphonenutzung erfasst. In allen drei Studien lag die Smartphonenutzung auf einem ähnlichen Niveau wie in der deutschen Referenzpopulation (95 %; Statista, 2019a). Darüber hinaus wurde die Kenntnis von vernetzten Automobilen vor der Teilnahme an den jeweiligen Studien erhoben. Das Bewusstsein für die

Existenz von vernetzten Automobilen war höher als Angaben vorangegangener Studien für eine deutsche Referenzpopulation (Federation internationale de l'automobile, 2016). Das höhere Bewusstsein könnte die fortschreitende Bekanntheit von vernetzen Automobilen in der breiten Gesellschaft wiederspiegeln, die durch zunehmende Marktverbreitung (Statista, 2019b) sowie eine erhöhte Medienpräsenz (Becker, 2017; dpa, 2018; Spaar, 2016) vorangetrieben wird. Tabelle 17 stellt die demographischen Variablen in den jeweiligen Studien 1-3 dieser Arbeit mit den Referenzwerten gegenüber. Die reine Kenntnis von vernetzten Automobilen ersetzt jedoch nicht die tatsächliche Erfahrung mit selbigen. Daher ist die Einbindung von Teilnehmenden ohne Erfahrung mit vernetzten Automobilen als Limitation dieser Arbeit zu verstehen, stellt jedoch gleichzeitig auch den Aufruf an kommende Studien dar, den Einfluss langfristiger Erfahrung mit vernetzten Diensten im Automobil zu beleuchten. Neben der mangelnden Langzeiterfahrung mit vernetzten Diensten im Automobil existieren mit der Privatheitskompetenz noch weitere möglicherweise konfundierende, personenbezogene Faktoren. Das Konstrukt der Privatheitskompetenz beschreibt das Wissen über die Rahmenbedingungen der Privatheit als auch das Wissen über Strategien im Umgang mit informationeller Privatheit (Trepte et al., 2015). Masur et al. (2017) schlagen mit der Online-Privatheitskompetenzskala ein fragebogenbasiertes Messinstrument zur Erfassung der Privatheitskompetenz im Online-Kontext vor. Auch wenn diese angesichts der oft geringen Bearbeitungsausdauer von Teilnehmenden in Online-Studien mit 20 Items recht umfangreich ausfällt, steht kommenden Studien mit dieser Skala ein validiertes und normiertes Instrument zur Erfassung und Kontrolle der Privatheitskompetenz zur Verfügung. Alternativ stellt das experimentelle Vorgehen von Keith et al. (2013), bei dem kritische konfundierende Variablen systematisch variiert wurden, eine gute Kontrollmöglichkeit für konfundierende Variablen dar.

Das bloße Stellen von privatheitsbezogenen Fragen kann bereits das Antwortverhalten der Teilnehmenden beeinflussen, da der Privatheitskontext dadurch salienter wird. Zwar ist dies eine Problematik, die der Privatheitsforschung inhärent zu sein scheint, da sie nahezu alle Studien betrifft. Dabei spielt auch diese Arbeit keine Ausnahme. Bloom et al. (2017) wendeten jedoch einen Ansatz an, der Primingeffekte durch das bloße Stellen von privatheitsbezogenen Fragen kontrollieren sollte. Bloom und Kollegen präsentierten nur der Hälfte der Teilnehmenden spezifische privatheitsbezogene Fragen, während alle Teilnehmende jedoch neben einer Fülle weiterer Fragen allgemeine privatheitsbezogene Fragen im Kontext von selbstfahrenden Automobilen beantworteten. Während somit etwaige Primingeffekte für die allgemeinen privatheitsbezogenen Fragen kontrolliert werden können, gilt dies jedoch nicht für die detaillierteren privatheitsbezogenen Fragen. Daher scheint auch das Verfahren von Bloom und Kollegen nicht

geeignet, um die Privatheit in verschiedenen Kontexten ohne etwaige Primingeffekte detailliert zu untersuchen.

Ursprünglich war es das Ziel die Modellschätzungen der drei Studien dieser Arbeit mittels einer Multigruppenanalyse direkt miteinander zu vergleichen. Wie zur Beantwortung von Forschungsfrage 2 in Studie 1 bereits angewandt, hat die Multigruppenanalyse im Rahmen der PLS-Modellierung den Vorteil einer inferenzstatistischen Aussagekraft. Allerdings erfüllten die drei Datensätze die für die Multigruppenanalyse notwendigen Bedingungen der Vergleichbarkeit nicht. Daher wurde auf eine deskriptive, vergleichende Analyse zurückgegriffen, wie sie in den ersten beiden Unterkapiteln der hiesigen Diskussion nachvollzogen werden kann.

In Kapitel 5.1.2 wurde die Sensitivität der preiszugebenden Daten mittels eines Expertenworkshops bestimmt, um auf dieser Basis die Rolle der Datensensibilität auf den Einfluss der privatheitsbezogenen Faktoren im Kontext von vernetzten Diensten im Automobil zu diskutieren. Betrachtet man allerdings neben der durch Experten gestützten Sensibilität der jeweiligen Datenpakte die Sensibilitätsscores auf Basis der subjektiven Bewertungen der einzelnen preiszugebenden Daten der Teilnehmenden, weichen letztere von diesem Erklärungsansatz ab. Hierzu wurden die individuellen Sensibilitätsbewertungen für alle Teilnehmenden in allen Studien von einem absoluten Wert in einen relativen Wert in Bezug zum Maximum des jeweiligen Sensibilitätsscores umgerechnet (d. h. in Prozent zum Maximum), sodass die Sensibilitätsscores trotz unterschiedlicher Maxima verglichen werden konnten. Um diese Beobachtung einordnen und interpretieren zu können, lohnt sich ein Blick auf das Fragebogendesign und den daraus folgenden Ablauf der jeweiligen Datenerhebung. Während die Bewertung der Modellfaktoren inklusive der Privatheitsbedenken sowie des Privatheitsrisikos auf Basis des kompletten preiszugebenden Datenpakets sowie im Kontext des jeweiligen vernetzten Dienstes im Automobil stattfand, basiert der Sensibilitätsscore auf der kontextbefreiten Bewertung einzelner Daten aus dem Datenpaket.

Bereits Westin (1967), aber ebenso Tavani und Moor (2001) betonten in ihren Konzeptualisierungen der Privatheit die Kontextabhängigkeit der selbigen. Die gleiche Handlung (zum Beispiel die Aufforderung zur Preisgabe bestimmter Informationen) kann in einem Kontext als privatheitskonform bewertet werden, während sie in einem anderen Kontext als eine Intrusion wahrgenommen wird. Entsprechend liegt der Bewertung einzelner Daten außerhalb eines jeglichen Kontextes mit einer hohen Wahrscheinlichkeit eine andere Bewertungsgrundlage zugrunde als der Betrachtung des preiszugebenden Datenpakets im Kontext des jeweiligen vernetzten Mehrwertdienstes im Automobil mit seinem kompletten Funktionsangebot.

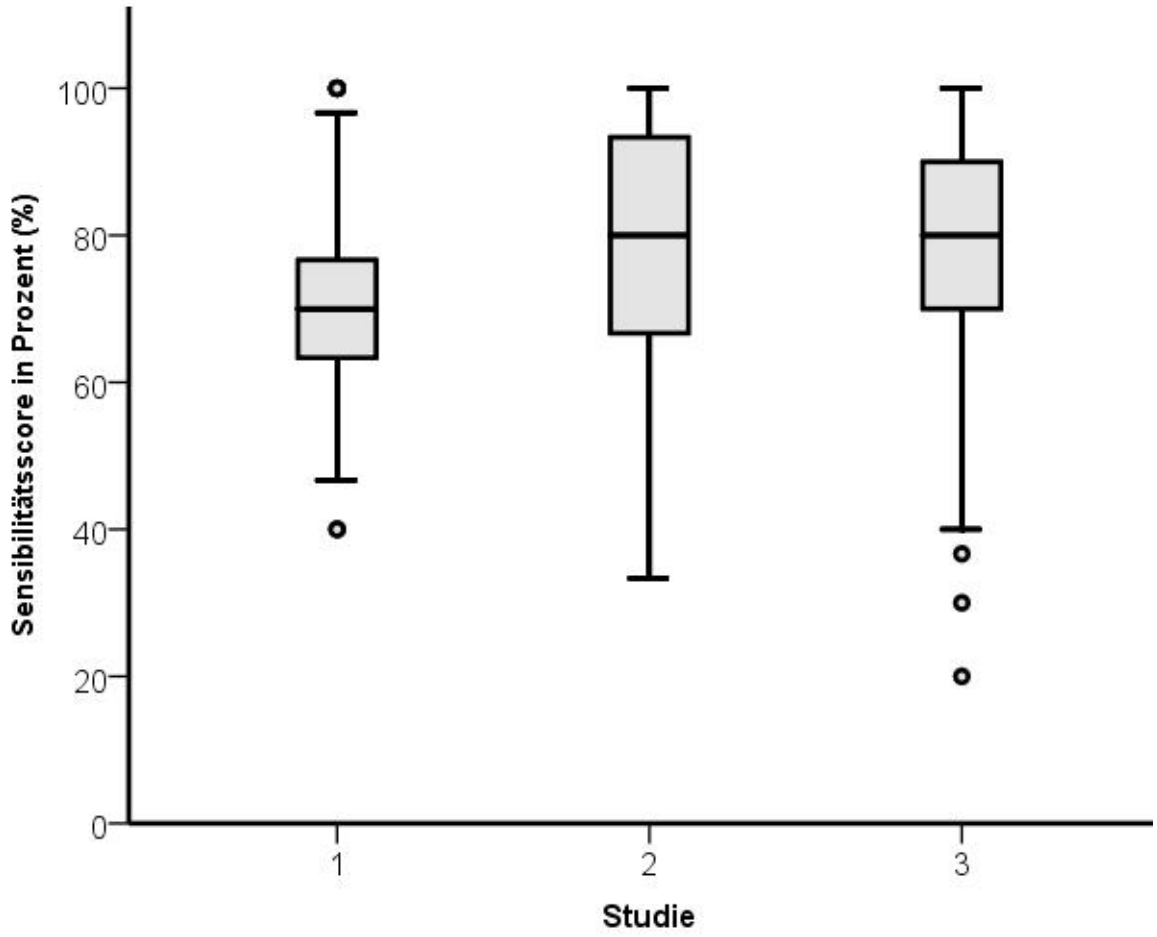


Abbildung 26. Vergleich der relativen Sensibilitätsscores in Prozent über die drei durchgeführten Studien hinweg.

Das Problem der kontextfremden Sensibilitätsbewertung wird ergänzt durch eine mögliche Nutzung der Bewertungsskala zur Differenzierung zwischen den abgefragten Datenpunkten. Vergleicht man die Sensibilitätsbewertungen des Standorts, der über alle drei Studien hinweg in den jeweiligen preiszugebenden Datenpaketen beinhaltet war, unterscheiden sich die Sensibilitätsbewertungen zwischen den Studien signifikant (Kruskal-Wallis-Test: χ^2 (2) = 14,47; $p <$ .05). Mann-Whitney-U post-hoc Tests zeigten, dass die Sensibilitätsbewertung des Standorts in Studie 2 (*Median* = 5,00) signifikant höher war als in den Studien 1 (*Median* = 4,00; $p <$ .05) und 3 (*Median* = 4,00; $p <$ .05). Obwohl das gleiche Datum bewertet wurde, fällt die Bewertung des Standorts in Studie 2 somit deutlich sensibler aus als in den anderen beiden Studien. Zieht man das jeweilige Datenpaket hinzu, dessen einzelne Daten im Anschluss an den Akzeptanzfragebogen bewertet wurden, kann dieser Unterschied durch die oben aufgeführte Differenzierung innerhalb der Datenpakte erklärt werden. Zwar wurden die einzelnen Daten vermutlich weiterhin außerhalb des Kontextes des vernetzten Dienstes bewertet. Die Teilnehmenden könnten jedoch, anders als intendiert, eine vergleichende Bewertung vorgenommen haben. Aus dem vergleichsweise wenig sensiblen Datenpaket des effizienzbezogenen Dienstes in Studie

2 sticht der Standort hervor und wird daher, im Vergleich zu den anderen preiszugebenden Daten, als besonders sensibel bewertet. Daher stellen sich die post-hoc Bewertungen der einzelnen preiszugebenden Daten als ungeeignet heraus, um durch die Berechnung eines Sensibilitätsscores auf die wahrgenommene Sensibilität des preiszugebenden Datenpakets zu schließen. Nur eine kontextbewusste Bewertung kann die wahrgenommene Sensibilität des preiszugebenden Datenpakets adäquat erfassen. Entsprechend können die Befunde bezüglich der prädiktiven Rolle des wahrgenommenen Privatheitsrisikos mit den kontextbewussten Expertenbewertungen der Sensibilität der jeweiligen preiszugebenden Datenpakete erklärt werden, während kein Zusammenhang mit den jeweiligen Sensibilitätsscores besteht.

5.4.2. Methodik Studie 1

Studie 1 ist die Hauptstudie dieser Thesis, der auch gleichzeitig das aufwändigste experimentelle Design zugrunde liegt. Aufgrund von organisatorischen Beschränkungen mussten beim Design der Studie jedoch Abwägungen getroffen werden, die hier erörtert werden.

Im Gegensatz zu den folgenden Studien 2 und 3 stellt Studie 1 eine Simulationsstudie dar, bei der Teilnehmende im Rahmen des Fahrsimulators des Instituts für Arbeitswissenschaft eine immersive Interaktionserfahrung mit einem vernetzten Dienst im Automobil sammeln konnten. Trotz der unternommenen Anstrengungen, um ein möglichst realistisches Szenario zu entwerfen, bleibt Studie 1 eine Simulationsstudie. Die Teilnehmenden könnten sich daher dem Simulationskontext bewusst gewesen sein. Die immersive Qualität der Simulationsstudie wurde mittels post-hoc Interviews überprüft. Die Interviews ergaben, dass keiner teilnehmenden Person in Studie 1 die Wizard-of-Oz Manipulationen im Zuge der Interaktion mit dem vernetzten Parkdienst auffiel. Alle Teilnehmenden waren der Überzeugung mit einem vollfunktionstüchtigen vernetzten Dienst zu interagieren. Darüber hinaus legen vorausgegangene Studien eine hohe Übertragbarkeit von Ergebnissen von Fahrsimulatorstudien auf das tatsächliche Verhalten im Straßenverkehr nahe (Bédard et al., 2010; Lee, 2003; Lee, H. C. et al., 2003).

Neben der Etablierung eines Akzeptanzmodells zur Erklärung der Nutzungsintention vernetzter Dienste im Automobil (Forschungsfrage 1) verfolgte Studie 2 auch das Ziel, den Einfluss einer tatsächlichen Interaktionserfahrung auf die Nutzungsintention eines vernetzten Dienstes im Automobil zu erfassen (Forschungsfrage 2). Während für die Etablierung des Akzeptanzmodells wichtig ist, dass alle Teilnehmenden vergleichbare Bedingungen für die Interaktion mit dem vernetzten Dienst vorfinden, sollten in einem within-subject Design wie im Fall von Studie 1 die experimentellen Bedingungen in ihrer Sequenz randomisiert werden, um Reihenfolgeeffekte ausschließen zu können. Damit widersprechen sich jedoch die Anforderungen der Etablierung des Akzeptanzmodells sowie des within-subject Designs. Während eine Randomisierung

der experimentellen Bedingungen ohne versus mit tatsächlicher Informationskontrolle den Anforderungen des within-subject Designs entsprochen hätte, hätte sie verhindert, dass alle Teilnehmenden mit in die Schätzung des Akzeptanzmodells mitaufgenommen werden können. Mögliche Lösungen scheinen zum einen die Verdopplung der Stichprobengröße im within-subject Designs inklusive der Randomisierung der experimentellen Bedingungen oder die Anwendung eines between-subject Design zu sein, sodass zum Beispiel $N_{between} = 232$ Teilnehmende an der Simulatorstudie teilgenommen hätten. Jeweils 116 Teilnehmende hätten die Parkplatzapplikation ohne (Gruppe 1) versus mit einer tatsächlichen Informationskontrolle (Gruppe 2) nutzen können. Die Rekrutierung von doppelt so vielen Teilnehmenden hätten einen immens höheren Ressourcenaufwand bedeutet. Vergleicht man die Stichprobengröße von Studie 1 mit anderen Simulatorstudien selbst im Kontext der Akzeptanzforschung (z. Bsp. Buckley et al., 2018; Hartwich et al., 2018) sticht diese bereits jetzt als große Stichprobe heraus. Daher wurde ein within-subject Design bevorzugt und damit einer höheren verwendbaren Stichprobengröße für die Etablierung des Akzeptanzmodells Vorrang gegeben.

Trotz dieser Einschränkungen ist Studie 1 eine der wenigen Studien, die sich mit experimentellen Manipulationen und der Möglichkeit zur tatsächlichen Interaktionserfahrung von der Mehrheit der Studien im Kontext der Akzeptanzforschung im Allgemeinen und unter Anwendung einer tatsächlichen Informationskontrolle im Speziellen abhebt (Gómez-Barroso, 2018).

6. Implikationen

Wie in vielen anderen Lebensbereichen hält die Digitalisierung und Vernetzung auch im Mobilitätskontext bereits seit einigen Jahren Einzug in das Automobil. Dabei bieten vernetzte Dienste im Automobil eine Vielzahl an positiven Neuerungen für individuelle Nutzende, Verkehrsteilnehmende im Allgemeinen sowie die beteiligten Unternehmen (Lee et al., 2016). Gleichzeitig hat die Vernetzung des Automobils über mehrere Disziplinen hinweg neue Forschungsfragen aufgeworfen, die derzeit noch Teil der aktuellen wissenschaftlichen Debatte sind. Diese Arbeit reiht sich ein in eine Vielzahl von anderen wissenschaftlichen Bemühungen, die Vernetzung sicherer und effizienter zu gestalten oder, wie in diesem Fall, die Gründe für eine hohe oder geringe Nutzungsintention angesichts der notwendigen Datenpreisgabe erklären zu können. Die Befunde dieser Arbeit haben sowohl für die Wissenschaft als auch für Praktiker wie Automobilhersteller oder –zulieferer sowie Anbieter von vernetzten Diensten im Automobil Implikationen, die in den beiden folgenden Kapiteln separat benannt werden.

Die Vernetzung im Allgemeinen und vernetzte Dienste im Speziellen stellen einen schnell wachsenden Kernabsatzmarkt im automobilen Kontext dar (Statista, 2019b). Entsprechend investieren Automobilhersteller hohe Summen, um die Vernetzung voranzutreiben und von ihr profitieren zu können (dpa, 2018). Die Ergebnisse dieser Arbeit können dabei helfen, dass die Resultate dieser Investitionen nicht an den Kunden vorbei zielen.

Einerseits bestätigt diese Arbeit das bereits bekannte Präferenzgefälle von sicherheits- über effizienz- bis hin zu komfortbezogenen Diensten. Darüber hinaus zeigen die hiesigen Ergebnisse jedoch auch, dass der Nutzen nicht unabhängig von den Kosten betrachtet werden kann. Die Nutzung eines bestimmten vernetzten Komfortfeatures mag unter der Bedingung einer niedrig sensiblen Datenpreisgabe angestrebt werden. Werden für das selbe Feature jedoch hoch sensible Daten eingefordert, kann dies zur Ablehnung des Features und somit zum Misserfolg eines vernetzten Dienstes führen. Daher wird hier die Relevanz eines privatheitsbewussten Designs von vernetzten Diensten im Automobil unterstrichen. Auf der Basis bekannter Nutzendenpräferenzen inklusive der Anerkennung der Relevanz des Schutzes ihrer Privatheit können Praktiker erfolgsversprechende vernetzte Dienste im Automobil entwerfen. Diese Arbeit zeigt im Speziellen die Relevanz der Informationskontrolle auf, sodass Dienstanbieter Maßnahmen ergreifen sollten, um eben diese in ihren Diensten gewährleisten zu können. Falls ausgeprägt führt die (wahrgenommene) Informationskontrolle letztendlich zu einer Erhöhung der Einstellung gegenüber der Nutzung des vernetzten Systems und / oder der Nutzungsintention, sodass durch sie auch die Interessen des Dienstanbieters unterstützt werden. Um sowohl den einflussreichen Privatheitsbedenken sowie dem wahrgenommenen Privatheitsrisiko entgegenzutreten, bieten

sich Entwicklern mit privacy-by-design und privacy-by-policy zwei Möglichkeiten um privatheitswahrende Dienste zu schaffen (Lederman et al., 2016). Durch die Implementierung mindestens einer dieser Ansätze in die Entwicklung vernetzter Dienste können Entscheidungsträger als auch Entwickler technische und organisatorische Maßnahmen nutzen um eine Datenverarbeitung sicherzustellen, die den Bedürfnissen der Nutzenden entgegenkommt. Motiviert werden solche Maßnahmen darüber hinaus auch durch aktuelle regulatorische Entwicklungen, wie sie in der Datenschutzgrundverordnung festgehalten werden. Die Vorgaben für die Etablierung eines privacy-by-design Prinzips gelten dabei auch für vernetzte Automobile (Plappert et al., 2017; Wachter, 2018). Sowohl die Bedürfnisse der Nutzenden als auch die Datenschutzgrundverordnung heben zwar die Relevanz eines privatheitsbewussten Vorgehens hervor, stellen sich der Entwicklung von vernetzten Diensten jedoch nicht in den Weg. Vielmehr stellen sie Leitplanken dar, die eine rechtskonforme und von den Nutzenden bevorzugte Gestaltungslösung ermöglichen. Dabei spielt die dargebotene Funktion trotz möglicher Datenschutzbedenken und –risiken noch immer eine prominente Rolle. Wie die obige Anwendung der Vorhersagen der hier etablierten Modelle am Beispiel des komfortbezogenen Dienstes zeigt, obliegt die Entscheidung bezüglich der Nutzung eines Dienstes einem Kosten-Nutzen-Trade-Off. Dies bedeutet jedoch neben allen Implikationen für die Relevanz der Privatheit bei der Nutzung von vernetzten Diensten im Automobil auch, dass nur attraktive Funktionen, die möglichst über ein einfach verständliches User Interface wahrgenommen werden können, die Nutzendengunst erobern können.

Im aktuellen Verkaufstrend von Automobilen nimmt der direkte Online-Verkauf von Neuwagen eine immer größere Rolle ein (Wittler, 2020). Während der klassische Erwerb eines Neuwagens über ein Autohaus die vorherige Interaktion mit dem Automobil im Allgemeinen, aber auch mit seinen (vernetzten) Diensten ermöglicht, fehlt diese Möglichkeit beim Online-Kauf. Anstelle von eigenen Interaktionserfahrungen werden videobasierte Informationen bereitgestellt. Ein Ansatz, der der Methodik der Studien 2 und 3 dieser Arbeit entspricht. Für beide Varianten lassen sich aus dieser Arbeit Empfehlungen für Automobilhersteller und Verkaufende ableiten. Besonders beim wachsenden Online-Verkauf sollten Automobilhersteller demnach ein besonderes Augenmerk auf das Vertrauensmanagement legen, während die Abschwächung von gegebenenfalls vorhandenen wahrgenommenen Privatheitsrisiken im Zentrum der Aufmerksamkeit von Verkaufenden im interaktionsbasierten Offline-Marketing liegen sollte. Die Ergebnisse dieser Arbeit legen nahe, dass die Integration einer einfachen Informationskontrolle eine vielversprechende Möglichkeit darstellt, Privatheitsbedenken und –risiken zu senken und eine Wahrscheinlichkeit der Nutzung des vernetzten Dienstes im Automobils zu erhöhen.

Unabhängig von dem angestrebten Vertriebsweg bietet darüber hinaus die Integration potentieller Nutzender bereits in frühen Phasen der Produktentwicklung die Möglichkeit, das Vertrauen in die Technologie zu stärken und die Verlässlichkeit von öffentlich-verfügbaren Informationen zu erhöhen (Zaunbrecher et al., 2016). Die Kombination einer transparenten, einfach zu erfassenden Kommunikation der Datenerfassung und –verarbeitung mit der Möglichkeit zu Hands-on Erfahrungen an Demonstratoren oder eben durch die Beteiligung an der Produktentwicklung schafft Vertrauen und schwächt Privatheitsbedenken ab, während eine zentrale Platzierung der Vorteile die Vorzüge des vernetzten Dienstes im Automobil hervorhebt. Beides sollte die öffentliche Kommunikationsstrategie von Automobilherstellern und Dienstanbietern prägen (Rohunen & Markkula, 2018).

7. Ausblick

Während in anderen datenintensiven Kontexten die Privatheitsrelevanz schon längst Einzug in die Akzeptanzmodellierung gehalten hat (Kim et al., 2017; Shevchuk et al., 2019; Yang et al., 2017), mangelte es bisher an einer entsprechenden Integration der zahlreichen Meinungs- und Präferenzumfragen zur Privatheit in vernetzten Automobilen. Diese Arbeit bietet mit dem hier aufgestellten und an verschiedenen vernetzten Diensten getesteten Akzeptanzmodell eine solide Grundlage für weitere Studien, die den Einfluss privatheitsrelevanter Faktoren im vernetzten Automobil untersuchen möchten. Dabei berücksichtigt das aufgestellte Akzeptanzmodell die bestehenden Befunde zu Privatheitsbedenken und wahrgenommenen Vorzügen von vernetzten Diensten im Automobil, bietet für diese jedoch auch gleichzeitig eine solide theoretische Struktur, um Bedenken, Überzeugungen und Einstellungen bezüglich vernetzter Dienste im Automobil in Verbindung zu setzen und genauer zu beleuchten. Ein besonderer Vorteil dieser Studie stellt die Fähigkeit des hier entwickelten Modells dar, Nutzungsintentionen erklären und vorhersagen zu können und somit die meist deskriptive Ebene bisheriger Erkenntnisse zu verlassen. Dabei lassen sich, wie in der obigen Diskussion bereits aufgezeigt, aus den hiesigen Befunden erste konkrete Aufgaben für weitere Forschung ableiten. Die Validierung des Modells an verschiedenen vernetzten Diensten über drei unterschiedliche Funktionsklassen hinweg ergab modelltheoretische Unterschiede, die durch Variationen in der Erfassung vorherigen Interaktionserfahrung, unterschiedlichen wahrgenommenen Nützlichkeiten sowie variierenden Datensensibilitäten erklärt werden konnten. Um die hiesigen Ergebnisinterpretationen weiter zu untermauern und das Zusammenspiel aus Datensensibilität, Nutzungserfahrung und unterschiedlich gewichteten Nutzen besser zu verstehen, können zukünftige Studien konkrete Studiendesigns aus dieser Arbeit ableiten. Ein mögliches Studienkonzept könnte zum Beispiel auf Basis des in Kapitel 5.1.2 aufgestellten Erklärungsansatzes auf einem 3x3x2-Studiendesign basieren, mit den abhängigen Variablen *Funktionsklasse* (komfortbezogen, effizienzbezogen, sicherheitsbezogen), *Güte der Informationen über den Anbieter* (Interaktionserfahrung; bloße Informationen über den Anbieter; keine Informationen) und *Datensensibilität des preiszugebenden Datenpakets* (niedrig versus hoch). In einem vollfaktorisierten Versuchsdesign könnten die hier aufgestellten Erklärungsansätze für den unterschiedlichen Einfluss von dem Vertrauen in den Anbieter, dem wahrgenommenen Privatheitsrisiko sowie die wahrgenommene Nützlichkeit weiterverfolgt und systematisch getestet werden.

Darüber hinaus liefert diese Arbeit Einblicke in die Auswirkungen der Erfassung von Akzeptanz versus Akzeptierbarkeit, die bisher konzeptionell unterschieden wurden (Nadal et al., 2019), deren praktische Auswirkungen aber dem Wissensstand des Autors entsprechend noch nicht

untersucht und verglichen wurden. Das oben vorgeschlagene Studienkonzept bietet dabei auch die Möglichkeit die unterschiedlichen Auswirkungen der Erfassung von Akzeptanz und Akzeptierbarkeit weiter systematisch zu beleuchten.

Während der Großteil der Forschung im Kontext des vernetzten Automobils technisch motiviert ist, liefert diese Arbeit eine modellbasierte, nutzendenzentrierte Perspektive auf das vernetzte Automobil. Daher können die hiesigen Ergebnisse auch als Aufruf an kommende Forschungsprojekte im Kontext des vernetzten Automobils verstanden werden, den in Kapitel 2.3.2 aufgeführten ersten Ansätzen zu folgen und interdisziplinäre Vorgehensweisen unter Einbeziehung der Nutzendenperspektive zu etablieren. Interessant wird dabei insbesondere die Betrachtung des Effekts von tatsächlichen Informationskontrollen auf das Nutzungs- und Preisgabeverhalten der Nutzenden sein.

Cavusoglu et al. (2016) zeigten, dass genauere, aber explizitere Kontrollmöglichkeiten einen differentiellen Effekt auf die Datenpreisgabe von Nutzenden haben. Personen, die bereits vorher über ein höheres Privatheitsbewusstsein verfügten, tendierten im Kontext von sozialen Netzwerken dazu unter dem Vorliegen von größeren Kontrollmöglichkeiten mehr Daten preiszugeben. Personen mit einem geringen a priori Privatheitsbewusstsein tendierten hingegen dazu, weniger Daten preiszugeben, obwohl die Kontrollmöglichkeiten nun besser waren. Durch die Privatheitskontrolle wurde die Privatheitsrelevanz für die weniger Privatheitsbewussten erst salient, sodass weniger Daten preisgegeben wurden. Aufgrund der vergleichsweise geringen Offensichtlichkeit der Vernetzung im Automobil ist eine Übertragbarkeit dieser Befunde auch auf den hiesigen Kontext vorstellbar. Zukünftige Studien können zum Beispiel unter Einsatz der Online-Privatheitskompetenzskala (Masur et al., 2017) die Angemessenheit dieser Vermutung genauer beleuchten.

8. Literaturverzeichnis

Acquisti, A., John, L. K. & Loewenstein, G. (2013, Juni). What Is Privacy Worth?, 249–274.

Ahmad, M. (2018). Review of The Technology Acceptance Model (TAM) in Internet banking and Mobile banking. *International Journal of Information Communication Technology and Digital Convergence*, *3*(1), 23–41.

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior. In J. Kuhl & J. Beckmann (Hg.), *Action Control: SSSP Springer Series in Social Psychology* (S. 11–39). Springer.

Ajzen, I. (1991). The Theory of Planned Behavior, 179–211.

Ajzen, I. & Driver, B. L. (1992). Application of the Theory of Planned Behavior to Leisure Choice. *Journal of Leisure Research*, *24*(3), 207–224. https://doi.org/10.1080/00222216.1992.11969889

Ajzen, I. & Fishbein, M. (1980). *Understanding attitudes and predicting social behavior*. Prentice.

Akalu, R. (2018). Privacy, consent and vehicular ad hoc networks (VANETs). *Computer Law & Security Review*, *34*(1), 37–46. https://doi.org/10.1016/j.clsr.2017.06.006

Allen, A. L. (1988). *Uneasy access: Privacy for women in a free society*. Rowman & Littlefield.

Al-Momani, A. M., Mahmoud, M. A. & Ahmad, M. S. (2019). A Review of Factors Influencing Customer Acceptance of Internet of Things Services. *International Journal of Information Systems in the Service Sector*, *11*(1), 54–67. https://doi.org/10.4018/IJISSS.2019010104

Alpers, S., Oberweis, A., Pieper, M., Betz, S., Fritsch, A., Schiefer, G. & Wagner, M. (2017). PRIVACY-AWARE: An Approach to Manage and Distribute Privacy Settings. In IEEE (Hg.), *3rd IEEE International Conference on Computer and Communications (ICCC): December 13-16, 2017, Chengdu, China* (S. 1460–1468). IEEE. https://avare.app/

Altman, I. (1975). *The environment and social behavior: privacy, personal space, territory, crowding*. Brooks.

Ando, R., Shima, S. & Takemura, T. (2016). Analysis of Privacy and Security Affecting the Intention of Use in Personal Data Collection in an IoT Environment. *IEICE Transactions on Information and Systems*, *E99.D*(8), 1974–1981. https://doi.org/10.1587/transinf.2015INI0002

Arcand, M., Nantel, J., Arles-Dufour, M. & Vincent, A. (2007). The impact of reading a web site's privacy statement on perceived control over privacy and perceived trust. *Online Information Review*, *31*(5), 661–681. https://doi.org/10.1108/14684520710832342

Askew, K., Buckner, J. E., Taing, M. U., Ilie, A., Bauer, J. A. & Coovert, M. D. (2014). Explaining cyberloafing: The role of the theory of planned behavior. *Computers in Human Behavior*, *36*, 510–519. https://doi.org/10.1016/j.chb.2014.04.006

Bagozzi, R. P., Wong, N., Abe, S. & Bergami, M. (2000). Cultural and Situational Contingencies and the Theory of Reasoned Action: Application to Fast Food Restaurant Consumption. *Journal of Consumer Psychology*, *9*(2), 97–106.

Bamberg, S. & Schmidt, P. (2003). Incentives, Morality, Or Habit? Predicting Students' Car Use for University Routes With the Models of Ajzen, Schwartz, and Triandis. *Environment and Behavior*, *35*(2), 264–285. https://doi.org/10.1177/0013916502250134

Bansal, G., Zahedi, F. "M." & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138–150. https://doi.org/10.1016/j.dss.2010.01.010

Bansal, P. & Kockelman, K. M. (2018). Are we ready to embrace connected and self-driving vehicles? A case study of Texans. *Transportation*, *45*(2), 641–675. https://doi.org/10.1007/s11116-016-9745-z

Bansal, P., Kockelman, K. M. & Singh, A. (2016). Assessing public opinions of and interest in new vehicle technologies: An Austin perspective. *Transportation Research Part C: Emerging Technologies*, *67*, 1–14. https://doi.org/10.1016/j.trc.2016.01.019

Baron, S., Patterson, A. & Harris, K. (2006). Beyond technology acceptance: understanding consumer practice. *International Journal of Service Industry Management*, *17*(2), 111–135. https://doi.org/10.1108/09564230610656962

Bauer, H. H., Schüle, A. & Toma, D. (2006). *Mehrwertorientierte Gestaltung mobiler Dienste im Fahrzeug: Eine empirische Untersuchung von Nutzeranforderungen* (Management Arbeitspapiere M104). Mannheim.

Beck, L. & Ajzen, I. (1991). Predicting Dishonest Actions Using the Theory of Planned Behavior. *Journal of Research in Personality*, *25*, 285–301.

Becker, J. (21. April 2017). Die Daten eines Autos sind das neue Öl. *Süddeutsche Zeitung,* 2017. https://www.sueddeutsche.de/auto/vernetzte-autos-die-daten-eines-autos-sind-das-neue-oel-1.3469344

Bédard, M., Parkkari, M., Weaver, B., Riendeau, J. & Dahlquist, M. (2010). Assessment of Driving Performance using a simulator protocol: Validity and reproducibility. *The American Journal of Occupational Therapy*, *64*(2), 336–340.

Beldad, A., Jong, M. de & Steehouder, M. (2010). How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. *Computers in Human Behavior*, *26*(5), 857–869. https://doi.org/10.1016/j.chb.2010.03.013

Berdigh, A. & Yassini, K. E. (2017). Connected car overview. In D. E. Boubiche, H. Hamdan & F. Hidoussi (Hg.), *ACM international conference proceedings series, IML'17: Proceedings of the International Conference on Internet of Things and Machine Learning : October 17-18, 2017, Liverpool John Moores University (LJMU), Liverpool city, United Kingdom* (S. 1–7). The Association for Computing Machinery. https://doi.org/10.1145/3109761.3158382

Beresford, A. R., Rice, A., Skehin, N. & Sohan, R. (2011). MockDroid: trading privacy for application functionality on smartphones. In L. Cox (Hg.), *Proceedings of the 12th Workshop on Mobile Computing Systems and Applications* (S. 49–54). ACM.

Berg, S. (2012). Einflussfaktoren der Nutzungsbereitschaft von Leistungsinnovationen auf Basis kontextsensitiver Telekommunikationsnetze bei Privatkunden in Deutschland: – Zwei empirische Untersuchungen zur Erkundung betriebswirtschaftlicher Absatzperspektiven für innovative mobilfunkbasierte Datendienste –, 1–185.

Bernsdorf, C., Hasreiter, N., Kranz, D., Sommer, S. & Rossmann, A. (2016). Technology Acceptance in the case of IoT Appliants, 49–63.

Bier, L., Joisten, P. & Abendroth, B. (2019). Warum nutzt der Mensch bevorzugt das Auto als Verkehrsmittel? Eine Analyse zum erlebten Fahrspaß unterschiedlicher Verkehrsmittelnutzer. *Zeitschrift für Arbeitswissenschaft*, *73*(1), 58–68. https://doi.org/10.1007/s41449-018-00144-9

Blau, P. (1964). *Power and exchange in social life.* John Wiley & Sons.

Bloom, C., Tan, J., Ramjohn, J. & Bauer, L. (2017). Self-Driving Cars and Data Collection: Privacy Perceptions of Networked Autonomous Vehicles: July 12-14, 2017, Santa Clara, CA, USA. In USENIX Association (Vorsitz), *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*. Symposium im Rahmen der Tagung von USENIX Association, Santa Clara.

BMW Group. (30. Mai 2017). *BMW Group startet BMW CarData: neue und innovative Services für den Kunden – sicher und transparent* [Press release]. https://www.press.bmwgroup.com/deutschland/article/detail/T0271366DE/bmw-group-startet-bmw-cardata:-neue-und-innovative-services-fuer-den-kunden-%E2%80%93-sicher-und-transparent?language=de

BMW Group. (2020). *BMW Connected Drive. FAQ.: Innovation beginnt mit Fragen. Hier finden Sie Antworten.* https://www.bmw-connecteddrive.de/app/index.html#/portal/faq-and-support?section=cardata

Bode, M. (2018). *Akzeptanz durch Selbstbestimmung – Eine Simulatorstudie zum vernetzten Fahrzeug* [Bachelorthesis]. Technische Universität Darmstadt, Darmstadt.

Boer, P. S. de, van Deursen, A. J.A.M. & van Rompay, T. J.L. (2019). Accepting the Internet-of-Things in our homes: The role of user skills. *Telematics and Informatics*, *36*, 147–156. https://doi.org/10.1016/j.tele.2018.12.004

Bok, S. (1983). *Secrets: On the Ethics of Concealment and Revelation*. Pantheon Books.

Bosler, M., Burr, W. & Ihring, L. (2019). Geschäftsmodell „Connected Car“ – digitale Innovationen in der Automobilindustrie. In S. Meinhardt & A. Pflaum (Hg.), *Edition HMD. Digitale Geschäftsmodelle: Geschäftsmodell-Innovationen, digitale Transformation, digitale Plattform, Internet der Dinge und Industrie 4.0* (Bd. 22, S. 73–96). Springer Vieweg. https://doi.org/10.1007/978-3-658-26316-4_5

Brandimarte, L., Acquisti, A. & Loewenstein, G. (2013). Misplaced Confidences: Privacy and the Control Paradox. *Social Psychological and Personality Science*, *4*(3), 340–347. https://doi.org/10.1177/1948550612455931

Brell, T., Biermann, H., Philipsen, R. & Ziefle, M. (2019). Conditional Privacy: Users' Perception of Data Privacy in Autonomous Driving. In O. Gusikhin & M. Helfert (Hg.), *Proceedings of the 5th International Conference on Vehicle Technology and Intelligent Transport Systems* (S. 352–359). SCITEPRESS - Science and Technology Publications. https://doi.org/10.5220/0007693803520359

Brell, T., Philipsen, R. & Ziefle, M. (2019). Suspicious minds? – users' perceptions of autonomous and connected driving. *Theoretical Issues in Ergonomics Science*, *9*(83), 1–31. https://doi.org/10.1080/1463922X.2018.1485985

Buck, C., Stadler, F., Suckau, K. & Eymann, T. (2017). Nutzer präferieren den Schutz ihrer Daten. *HMD Praxis der Wirtschaftsinformatik*, *54*(1), 55–66. https://doi.org/10.1365/s40702-016-0280-3

Buckley, L., Kaye, S.-A. & Pradhan, A. K. (2018). Psychosocial factors associated with intended use of automated vehicles: A simulated driving study. *Accident; analysis and prevention*, *115*, 202–208. https://doi.org/10.1016/j.aap.2018.03.021

Carminati, B., Colombo, P., Ferrari, E. & Sagirlar, G. (2016). Enhancing User Control on Personal Data Usage in Internet of Things Ecosystems. In J. Zhang, J. A. Miller & X. Xu (Hg.), *2016 IEEE International Conference on Services Computing: SCC 2016 : 27 June-2 July 2016, San Francisco, California, USA : proceedings* (S. 291–298). IEEE. https://doi.org/10.1109/SCC.2016.45

Cavusoglu, H., Phan, T. Q., Cavusoglu, H. & Airoldi, E. M. (2016). Assessing the Impact of Granular Privacy Controls on Content Sharing and Disclosure on Facebook. *Information Systems Research*, *27*(4), 848–879.

Chen, C. D., Fan, Y. W. & Farn, C. K. (2007). Predicting electronic toll collection service adoption: An integration of the technology acceptance model and the theory of planned behavior. *Transportation Research Part C: Emerging Technologies*, *15*(5), 300–311.

Chen, H. H. & Chen, S. C. (2009). The empirical study of automotive telematics acceptance in Taiwan: comparing three Technology Acceptance Models. *International Journal of Mobile Communications*, *7*(1), Artikel 21672, 50. https://doi.org/10.1504/IJMC.2009.021672

Chesney, T. (2006). An Acceptance Model for useful and fun information systems. *Human Technology*, *2*(2), 225–235.

Chung, J. E., Park, N., Wang, H., Fulk, J. & McLaughlin, M. (2010). Age differences in perceptions of online community participation among non-users: An extension of the Technology Acceptance Model. *Computers in Human Behavior*, *26*(6), 1674–1684.

Cohen, J. (1992). A power primer. *Psychological Bulletin*, *112*(1), 155–159.

Coppola, R. & Morisio, M. (2016). Connected Car. *ACM Computing Surveys*, *49*(3), 1–36. https://doi.org/10.1145/2971482

Cottrill, C. D. & Thakuriah, P. (2015). Location privacy preferences: A survey-based analysis of consumer awareness, trade-off and decision-making. *Transportation Research Part C: Emerging Technologies*, *56*, 132–148. https://doi.org/10.1016/j.trc.2015.04.005

Crabtree, A., Lodge, T., Colley, J., Greenghalgh, C. & Mortier, R. (2017). Accountable Internet of Things? Outline of the IoT databox model. In *18th IEEE International Symposium on a World of Wireless, Mobile, and Multimedia Networks (WoWMoM 2017): June 12-15, 2017, Macao Polytechnic Institute* (S. 1–6). IEEE. https://doi.org/10.1109/WoWMoM.2017.7974335

Culnan, M. J. & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. https://doi.org/10.1287/orsc.10.1.104

Cunningham, S. M. (1967). The major dimensions of perceived risk. In D. F. Cox (Hg.), *Risk taking and information handling in consumer behavior.* Havard University Press.

Dakroub, H., Shaout, A. & Awajan, A. (2016). Connected Car Architecture and Virtualization. *SAE International Journal of Passenger Cars - Electronic and Electrical Systems*, *9*(1), 153–159. https://doi.org/10.4271/2016-01-0081

Danezis, G., Lewis, S. & Andersson, R. (2005). How Much is Location Privacy Worth?, 1–13.

Dao, V. D. (2017). *Entwicklung und Umsetzung einer virtuellen Fahrumgebung im Fahrsimulator* [Bachelor-Thesis]. Technische Universität Darmstadt, Darmstadt.

Davis, F. D. (1986). *A technology acceptance model for empirically testing new end-user information systems: Theory and results* [Dissertation]. Massachusetts Insitute of Technology, Cambridge.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319. https://doi.org/10.2307/249008

Davis, F. D., Bagozzi, R. P. & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *Vol. 35*(No. 8), 982–1003.

Deloitte. (2015). *Connected Car - Generation Y und die nächste Generation des Automobils*. https://www2.deloitte.com/content/dam/Deloitte/de/Documents/manufacturing/150909_DEL-15-5015_Brosch%C3%BCre_DasConnectedCar_rz_WEB-safe.pdf

Derikx, S., Reuver, M. de & Kroesen, M. (2016). Can privacy concerns for insurance of connected cars be compensated? *Electronic Markets*, *26*(1), 73–81. https://doi.org/10.1007/s12525-015-0211-0

Dienlin, T. (2014). The privacy process model. In S. Garnett, S. Halft, M. Herz, & J.-M. Mönig (Hg.), *Medien und Privatheit* (S. 105–122). Stutz.

Dietzel, S., Kosty, M., Schaubz, F. & Kargl, F. (2012). CANE: A controlled application environment for privacy protection in ITS. In J.-C. Lin (Vorsitz), *12th International Conference on ITS Telecommunications*. Symposium im Rahmen der Tagung von IEEE Communications Society, Taipei, Taiwan.

Dinev, T. & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. https://doi.org/10.1287/isre.1060.0080

Distler, V., Lallemand, C. & Bellet, T. (2018). Acceptability and Acceptance of Autonomous Mobility on Demand. In R. Mandryk & M. Hancock (Hg.), *Engage with CHI: CHI 2018 : proceedings of the 2018 CHI Conference on Human Factors in Computing Systems : April 21 -26, 2018, Montréal, QC, Canada* (S. 1–10). The Association for Computing Machinery. https://doi.org/10.1145/3173574.3174186

dpa (9. März 2014). "Das Auto darf nicht zur Datenkrake werden": VW-Chef zur Cebit-Eröffnung. *Spiegel,* 2014. https://www.spiegel.de/netzwelt/netzpolitik/cebit-vw-chef-martin-winterkorn-warnt-vor-auto-als-datenkrake-a-957753.html

dpa (23. August 2018). Volkswagen: Milliarden-Investition in Vernetzung. dpa. https://www.heise.de/autos/artikel/Volkswagen-Milliarden-Investition-in-Vernetzung-4144438.html

Du, S., Keil, M., Mathiassen, L., Shen, Y. & Tiwana, A. (2006). The Role of Perceived Control, Attention-Shaping, and Expertise in IT Project Risk Assessment. In R. H. Sprague (Hg.), *Proceedings of the 39th Annual Hawaii International Conference on System Sciences, 2006, HICSS '06: 04 - 07 Jan. 2006, [Kauai, Hawaii* (192c-192c). IEEE Computer Society. https://doi.org/10.1109/HICSS.2006.483

Dwyer, C., Hiltz, S. & Passerini, K. (2007). Trust and privacy concern within social networking sites: A comparison of Facebook and MySpace. *AMCIS 2007 proceedings*, 339.

Ebeling, C. (2018). *Selbstbestimmt vernetzt fahren - Eine Simulatorstudie zum vernetzten Fahrzeug* [Masterthesis]. Technische Universität Darmstadt, Darmstadt.

Ellaway, A., Macintyre, S., Hiscock, R. & Kearns, A. (2003). In the driving seat: psychosocial benefits from private motor vehicle transport compared to public transport. *Transportation Research Part F: Traffic Psychology and Behaviour*, *6*(3), 217–231. https://doi.org/10.1016/S1369-8478(03)00027-5

El-Rewini, Z., Sadatsharan, K., Selvaraj, D. F., Plathottam, S. J. & Ranganathan, P. (2020). Cybersecurity challenges in vehicular communications. *Vehicular Communications*, *23*, 100214. https://doi.org/10.1016/j.vehcom.2019.100214

Emami-Naeini, P., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F. & Sadeh, N. (2006). Privacy Expectations and Preferences in an IoT World. In USENIX Association (Hg.), *Proceedings of SOUPS 2006, Symposium on Usable Privacy and Security* (S. 399–412). USENIX Association.

Endo, T., Nawa, K., Kato, N. & Murakami, Y. (2016). Study on privacy setting acceptance of drivers for data utilization on connected cars. In S. a. T. Annual Conference on Privacy (Hg.), *2016 14th Annual Conference on Privacy, Security and Trust (PST): 12-14 Dec. 2016* (S. 82–87). IEEE. https://doi.org/10.1109/PST.2016.7906941

Eriksson, L. & Bjørnskau, T. (2012). Acceptability of traffic safety measures with personal privacy implications. *Transportation Research Part F: Traffic Psychology and Behaviour*, *15*(3), 333–347. https://doi.org/10.1016/j.trf.2012.02.006

Verordnung (EU) 2015/758 über Anforderungen für die Typgenehmigung zur Einführung des auf dem 112-Notruf basierenden bordeigenen eCall-Systems in Fahrzeugen und zur Änderung der Richtlinie 2007/46/EG 77 (2015 & i.d.F.v. Deutsch). https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX%3A32015R0758

Regulation (EU) 2016/ 679 - on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95 / 46 / EC (General Data Protection Regulation), Official Journal of the European Union 1 (2016).

Evjemo, B., Castejón-Martínez, H. & Akselsen, S. (2018). Trust trumps concern: Findings from a seven-country study on consumer consent to 'digital native' vs. 'digital immigrant' service providers. *Behaviour & Information Technology*, *38*(5), 503–518. https://doi.org/10.1080/0144929X.2018.1541254

Eyssartier, C. (2015). Acceptability of driving an equipped vehicle with drive recorder: the impact of the context. *IET Intelligent Transport Systems*, *9*(7), 710–715. https://doi.org/10.1049/iet-its.2014.0174

Fazel, L. (2014). *Akzeptanz von Elektromobilität*. Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-05090-0

Fazio, R. H. (1990). Multiple Processes by which attitudes guide behavior: The MODE model as an integrative framework. *Advances in Experimental Social Psychology*, *23*, 75–109.

Featherman, M. S., Miyazaki, A. D. & Sprott, D. E. (2010). Reducing online privacy risk to facilitate e-service adoption: the influence of perceived ease of use and corporate credibility. *Journal of Services Marketing*, *24*(3), 219–229. https://doi.org/10.1108/08876041011040622

Federation internationale de l'automobile. (2016). *What Europeans think about connected cars.* FIA Region I. www.mycarmydata.eu

Fishbein, M. & Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Addison-Wesley.

Floridi, L. (2005). The Ontological Interpretation of Informational Privacy. *Ethics and Information Technology*, *7*(4), 185–200. https://doi.org/10.1007/s10676-006-0001-7

Fornell, C. & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of marketing research*, *18*(1), 39–50.

Friginal, J., Gambs, S., Guiochet, J. & Killijian, M.-O. (2014). Towards privacy-driven design of a dynamic carpooling system. *Pervasive and Mobile Computing*, *14*, 71–82. https://doi.org/10.1016/j.pmcj.2014.05.009

Frye, N. E. & Dornisch, M. M. (2010). When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior*, *26*(5), 1120–1127. https://doi.org/10.1016/j.chb.2010.03.016

Gao, L., Wang, S., Li, J. & Li, H. (2017). Application of the extended theory of planned behavior to understand individual's energy saving behavior in workplaces. *Resources, Conservation and Recycling*, *127*, 107–113. https://doi.org/10.1016/j.resconrec.2017.08.030

Gao, L. & Bai, X. (2014). A unified perspective on the factors influencing consumer acceptance of internet of things technology. *Asia Pacific Journal of Marketing and Logistics*, *26*(2), 211–231. https://doi.org/10.1108/APJML-06-2013-0061

Gardner, B. & Abraham, C. (2007). What drives car use? A grounded theory analysis of commuters' reasons for driving. *Transportation Research Part F: Traffic Psychology and Behaviour*, *10*(3), 187–200. https://doi.org/10.1016/j.trf.2006.09.004

Gefen, D., Karahanna, E. & Straub, D. W. (2003). Trust and TAM in online shopping: an integrated model. *MIS Quarterly*, *27*(1), 51–90.

Gefen, D., Rao, V. S. & Tractinsky, N. (2003). The conceptualization of trust, risk and their relationship in electronic commerce: The need for clarifications. In IEEE Computer Society (Vorsitz), *HICSS '03*. Symposium im Rahmen der Tagung von IEEE Computer Society, Hawaii.

Ghazizadeh, M., Lee, J. D. & Boyle, L. N. (2012). Extending the Technology Acceptance Model to assess automation. *Cognition, Technology & Work*, *14*(1), 39–49. https://doi.org/10.1007/s10111-011-0194-3

Ghazizadeh, M., Peng, Y., Lee, J. D. & Boyle, L. N. (2012). Augmenting the Technology Acceptance Model with Trust: Commercial Drivers' Attitudes towards Monitoring and Feedback. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *56*(1), 2286–2290. https://doi.org/10.1177/1071181312561481

Gideon, J., Egelman, S., Cranor, L. F. & Acquisti, A. (2006). Power Strips, Prophylactics, and Privacy, Oh My! In USENIX Association (Hg.), *Proceedings of SOUPS 2006, Symposium on Usable Privacy and Security* (S. 133–144). USENIX Association.

Godin, G. & Kok, G. (1996). The Theory of Planned Behavior: A Review of its Appications to Health-related Behaviors. *Behavior Change*, *11*(2), 87–98.

Golias, J., Yannis, G. & Antoniou, C. (2002). Classification of driver-assistance systems according to their impact on road safety and traffic efficiency. *Transport Reviews*, *22*(2), 179–196.

Gómez-Barroso, J. L. (2018). Experiments on personal information disclosure: Past and future avenues. *Telematics and Informatics*, *35*(5), 1473–1490. https://doi.org/10.1016/j.tele.2018.03.017

Goodhue, D. L., Lewis, W. & Thompson, R. (2012). Does PLS have advantages for small sample size or non-normal data? *MIS Quarterly*, *36*(3).

Groll, A., Holle, J., Ruland, C., Wolf, M., Wollinger, T. & Zweers, F. (2009). OVERSEE. A Secure and Open Communication and Runtime Platform for Innovative Automotive Applications. In istis AG (Vorsitz), *ESCAR - Embedded security in cars,* Düsseldorf, Germany.

Gründl, M. (2005). *Fehler und Fehlverhalten als Ursache von Verkehrsunfällen und Konsequenzen für das Unfallvermeidungspotenzial und die Gestaltung von Fahrerassistenzsystemen* [Dissertation]. Universität Regensburg, Regensburg.

Gu, J., Xu, Y., Xu, H., Zhang, C. & Ling, H. (2017). Privacy concerns for mobile app download: An elaboration likelihood model perspective. *Decision Support Systems*, *94*, 19–28. https://doi.org/10.1016/j.dss.2016.10.002

Hair, J. F., Hult, G. T. M., Ringle, C. & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage publications.

Hair, J. F., Ringle, C. M. & Sarstedt, M. (2011). PLS-SEM: Indeed a Silver Bullet. *Journal of Marketing Theory and Practice*, *19*(2), 139–152. https://doi.org/10.2753/MTP1069-6679190202

Hajli, N. & Lin, X. (2016). Exploring the Security of Information Sharing on Social Networking Sites: The Role of Perceived Control of Information. *Journal of Business Ethics*, *133*(1), 111–123. https://doi.org/10.1007/s10551-014-2346-x

Hang, A., Zezschwitz, E. von, Luca, A. de & Hussmann, H. (2012). Too much Information! User Attitudes towards Smartphone Sharing. In L. Malmborg (Hg.), *Proceedings of the 7th Nordic Conference on Human-Computer Interaction Making Sense Through Design* (S. 284–287). ACM.

Hansen, M. (2015). Das Nezt im Auto & das Auto im Netz. *Datenschutz und Datensicherheit*(6), 367–371.

Hartwich, F., Beggiato, M. & Krems, J. F. (2018). Driving comfort, enjoyment and acceptance of automated driving – effects of drivers' age and driving style familiarity. *Ergonomics*, *61*(8), 1017–1032. https://doi.org/10.1080/00140139.2018.1441448

He, W., Yan, G. & Xu, L. D. (2014). Developing Vehicular Data Cloud Services in the IoT Environment. *IEEE Transactions on Industrial Informatics*, *10*(2), 1587–1595. https://doi.org/10.1109/TII.2014.2299233

Hegner, S. M., Beldad, A. D. & Brunswick, G. J. (2019). In Automatic We Trust: Investigating the Impact of Trust, Control, Personality Characteristics, and Extrinsic and Intrinsic Motivations on the Acceptance of Autonomous Vehicles. *International Journal of Human–Computer Interaction*, *35*(19), 1769–1780. https://doi.org/10.1080/10447318.2019.1572353

Henseler, J., Ringle, C. M. & Sarstedt, M. (2016). Testing measurement invariance of composites using partial least squares. *International Marketing Review*, *33*(3), 405–431. https://doi.org/10.1108/IMR-09-2014-0304

Horswill, M. S. & McKenna, F. P. (1999). The Effect of Perceived Control on Risk Taking. *Journal of Applied Social Psychology*, *29*(2), 377–391.

Hsiao, C. H. & Yang, C. (2011). The intellectual development of the technology acceptance model: A co-citation analysis. *International Journal of Information Management*, *31*(2), 128–136. https://doi.org/10.1016/j.ijinfomgt.2010.07.003

Hsu, C.-L. & Lin, J. C.-C. (2016). An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior*, *62*, 516–527. https://doi.org/10.1016/j.chb.2016.04.023

Huang, S.-C., Chen, B.-H., Chou, S.-K., Hwang, J.-N. & Lee, K.-H. (2016). Smart Car. *IEEE Computational Intelligence Magazine*, *11*(4), 46–58. https://doi.org/10.1109/MCI.2016.2601758

Hussain, S. U. & Koushanfar, F. (2018). P3: Privacy Preserving Positioning for Smart Automotive Systems. *ACM Transactions on Design Automation of Electronic Systems*, *23*(6), 1–19. https://doi.org/10.1145/3236625

ISO (2011). *Ergonomics of human-system interaction. Part 210: Human-centred design process for interactive systems*. Geneva. ISO.

ISO (2019). *ISO 20078-1:2019*.

Johanning, V. & Mildner, R. (2015). *Car IT kompakt: Das Auto der Zukunft – Vernetzt und autonom fahren* (1. Aufl.). Springer Fachmedien Wiesbaden.

Joy, J. & Gerla, M. (2017). Internet of vehicles and autonomous connected car -privacy and security issues. In IEEE Computer Society (Vorsitz), *ICCCN 2017*. Symposium im Rahmen der Tagung von IEEE Computer Society, Vancouver, Canada.

Karaboga, M., Matzner, T., Morlok, T., Pittroff, F., Nebel, M., Ochs, C., Pape, T. von, Pörschke, J. V., Schütz, P. & Fhom, H. S. (2015). *Das versteckte Internet: Zu Hause - Im Auto - Am Körper*. Forum Privatheit.

Karnouskos, S. & Kerschbaum, F. (2018). Privacy and Integrity Considerations in Hyperconnected Autonomous Vehicles. *Proceedings of the IEEE*, *106*(1), 160–170. https://doi.org/10.1109/JPROC.2017.2725339

Kazakevičiūtė, A. & Banytė, J. (2013). The Relationship of Consumers‘ Perceived Hedonic Value and Behavior. *Engineering Economics*, *23*(5). https://doi.org/10.5755/j01.ee.23.5.1975

Kraftfahrtbundesamt. (2. März 2020). *Der Fahrzeugbestand am 1. Januar 2020* [Press release]. Flensburg.

Keith, M. J., Maynes, C., Lowry, P. B. & Babb, J. (2014). “Privacy fatigue: The effect of privacy control complexity on consumer electronic information disclosure. In AIS (Vorsitz), *ICIS 2014,* Auckland, New Zeeland.

Keith, M. J., Thompson, S. C., Hale, J., Lowry, P. B. & Greer, C. (2013). Information disclosure on mobile devices: Re-examining privacy calculus with actual user behavior. *International Journal of Human-Computer Studies*, *71*(12), 1163–1173. https://doi.org/10.1016/j.ijhcs.2013.08.016

Kelkel, R. (2015). *Predicting consumers’ intention to purchase fully autonomous driving systems – Which factors drive acceptance?* [Master Thesis].

Keuntje, P. & Poormohammadroohafza, F. (2014). *Car Infotainment: An early analysis of driver perceptions towards apps in the car* [Masterthesis]. Lund University, Lund.

Kim, Y., Park, Y. & Choi, J. (2017). A study on the adoption of IoT smart home service: using Value-based Adoption Model. *Total Quality Management & Business Excellence*, *28*(9-10), 1149–1165. https://doi.org/10.1080/14783363.2017.1310708

Klumpp, M. & Schmitt, R. (2018). *Vernetztes Fahren im Kontext der Datenpreisgabe – Durchführung und Auswertung einer Simulatorstudie im IAD-Fahrsimulator* [Tutorium]. Technische Universität Darmstadt, Darmstadt.

Kowatsch, T. & Maass, W. (2012). Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts. In H. Rahman, A. Mesquita, I. Ramos & B. Pernici (Hg.), *Lecture Notes in Business Information Processing: Bd. 129. Knowledge and Technologies in Innovative Information Systems: 7th Mediterranean Conference on Information Systems, MCIS 2012, Guimaraes, Portugal, September 8-10, 2012. Proceedings* (Bd. 129, S. 200–211). Springer. https://doi.org/10.1007/978-3-642-33244-9_14

Krasnova, H., Spiekermann, S., Koroleva, K. & Hildebrand, T. (2010). Online Social Networks: Why We Disclose. *Journal of Information Technology*, *25*(2), 109–125. https://doi.org/10.1057/jit.2010.6

Krauß, C. & Waidner, M. (2015). IT-Sicherheit und Datenschutz im vernetzten Fahrzeug: Bedrohungen und Herausforderungen. *Datenschutz und Datensicherheit*(6), 383–387.

Kulviwat, S., Bruner II, G. C., Kumar, A., Nasco, S. A. & Clark, T. (2007). Toward a unified theory of consumer acceptance technology. *Psychology and Marketing*, *24*(12), 1059–1084. https://doi.org/10.1002/mar.20196

Kung, A., Raither, B. & Kost, M. (2011). *Guidelines for Privacy Aware Cooperative Application* (v1.2). PRECIOSA.

Larue, G. S., Rakotonirainy, A., Haworth, N. L. & Darvell, M. (2015). Assessing driver acceptance of Intelligent Transport Systems in the context of railway level crossings. *Transportation Research Part F: Traffic Psychology and Behaviour*, *30*, 1–13. https://doi.org/10.1016/j.trf.2015.02.003

Laufer, R. S. & Wolfe, M. (1977). Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, *33*(3), 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x

Lederman, J., Taylor, B. D. & Garrett, M. (2016). A private matter: the implications of privacy regulations for intelligent transportation systems. *Transportation Planning and Technology*, *39*(2), 115–135. https://doi.org/10.1080/03081060.2015.1127537

Lee, E.-K., Gerla, M., Pau, G., Lee, U. & Lim, J.-H. (2016). Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs. *International Journal of Distributed Sensor Networks*, *12*(9). https://doi.org/10.1177/1550147716665500

Lee, H. S. "A.", Lambert, C. U. & Law, R. (2011). The Relationship of Perceived Cognitive and Decisional Controls in Information Disclosure: Decomposition of Perceived Control. *International Journal of Tourism Sciences*, *11*(1), 53–74. https://doi.org/10.1080/15980634.2011.11434635

Lee, H. (2003). The Validity of Driving Simulator to Measure On-Road Driving Performance of Older Drivers. *Transport Engineering in Australia*, *8*(2), 89.

Lee, H. C., Cameron, D. & Lee, A. H. (2003). Assessing the driving performance of older adult drivers: on-road versus simulated driving. *Accident Analysis & Prevention*, *35*(5), 797–803. https://doi.org/10.1016/S0001-4575(02)00083-0

Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research and Applications*, *8*(3), 130–141. https://doi.org/10.1016/j.elerap.2008.11.006

Lee, W. & Shin, S. (2019). An Empirical Study of Consumer Adoption of Internet of Things Services. *International Journal of Engineering and Technology Innovation*, *9*(1), 1–11.

Lee, Y., Kozar, K. A. & Larsen, K. R.T. (2003). The Technology Acceptance Model: Past, Present, and Future. *Communications of the Association for Information Systems*, *12*. https://doi.org/10.17705/1CAIS.01250

Legris, P., Ingham, J. & Collerette, P. (2003). Whay do people use information technology? A critical review of the technology acceptance model. *Information & Management*, *40*, 191–204.

Leiner, D. J. (2019). Too Fast, too Straight, too Weird: Non-Reactive Indicators for Meaningless Data in Internet Surveys. Advance online publication. https://doi.org/10.18148/SRM/2019.V13I3.7403 (229-248 Pages / Survey Research Methods, Vol 13 No 3 (2019) / Survey Research Methods, Vol 13 No 3 (2019)).

Leung, L. & Chen, C. (2017). Extending the theory of planned behavior: A study of lifestyles, contextual factors, mobile viewing habits, TV content interest, and intention to adopt mobile TV. *Telematics and Informatics*, *34*(8), 1638–1649. https://doi.org/10.1016/j.tele.2017.07.010

Li, P., Cho, H. & Goh, Z. H. (2019). Unpacking the process of privacy management and self-disclosure from the perspectives of regulatory focus and privacy calculus. *Telematics and Informatics*, *41*, 114–125. https://doi.org/10.1016/j.tele.2019.04.006

Lim, H. & Taeihagh, A. (2018). Autonomous Vehicles for Smart and Sustainable Cities: An In-Depth Exploration of Privacy and Cybersecurity Implications. *Energies*, *11*(5), 1062. https://doi.org/10.3390/en11051062

Lin, J., Liu, B., Sadeh, N. & Hong, J. I. (2014). Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings. In USENIX Association (Vorsitz), *Tenth Symposium On Usable Privacy and Security*. Symposium im Rahmen der Tagung von USENIX Association, Menlo Park, CA, USA.

Liu, B., Lin, J. & Sadeh, N. (2014). Reconciling mobile app privacy and usability on smartphones. In C.-W. Chung (Hg.), *Proceedings of the 23rd International Conference on World Wide Web: April 7 - 11, 2014, Seoul, Korea* (S. 201–212). ACM Press. https://doi.org/10.1145/2566486.2568035

Lowry, P. B., Cao, J. & Everard, A. (2011). Privacy Concerns Versus Desire for Interpersonal Awareness in Driving the Use of Self-Disclosure Technologies: The Case of Instant Messaging in Two Cultures. *Journal of Management Information Systems*, *27*(4), 163–200. https://doi.org/10.2753/MIS0742-1222270406

MacKinnon, D. P., Fairchild, A. J. & Fritz, M. S. (2007). Mediation analysis. *Annual review of psychology*, *58*, 593–614. https://doi.org/10.1146/annurev.psych.58.110405.085542

Madigan, R., Louw, T., Wilbrink, M., Schieben, A. & Merat, N. (2017). What influences the decision to use automated public transport? Using UTAUT to understand public acceptance

of automated road transport systems. *Transportation Research Part F: Traffic Psychology and Behaviour*, *50*, 55–64.

Madigan, R., Louw, T., Dziennus, M., Graindorge, T., Ortega, E., Graindorge, M. & Merat, N. (2016). Acceptance of Automated Road Transport Systems (ARTS): An Adaptation of the UTAUT Model. *Transportation Research Procedia*, *14*, 2217–2226. https://doi.org/10.1016/j.trpro.2016.05.237

Mahlke, S. (2005). Understanding users' experience of interaction. In N. Marmaras & T. Kontogiannis (Vorsitz), *Annual conference on European association of cognitive ergonomics.* Symposium im Rahmen der Tagung von ACM, Athen, Griechenland.

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society*, *32*(3), 192–199. https://doi.org/10.1080/01972243.2016.1153010

Makhdoom, I., Zhou, I., Abolhasan, M., Lipman, J. & Ni, W. (2020). PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities. *Computers & Security*, *88*, 101653. https://doi.org/10.1016/j.cose.2019.101653

Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004a). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Malhotra, N. K., Kim, S. S. & Agarwal, J. (2004b). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Marangunić, N. & Granić, A. (2015). Technology acceptance model: a literature review from 1986 to 2013. *Universal Access in the Information Society*, *14*(1), 81–95. https://doi.org/10.1007/s10209-014-0348-1

Margulis, S. T. (1977). Conceptions of Privacy: Current Status and Next Steps. *Journal of Social Issues*, *33*(3), 5–21.

Margulis, S. T. (2003). On the Status and Contribution of Westin's and Altman's Theories of Privacy. *Journal of Social Issues*, *59*(2), 411–429.

Margulis, S. T. (2011). Three Theories of Privacy: An Overview. In S. Trepte & L. Reinecke (Hg.), *Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web* (S. 9–17). Springer.

Martin, N., Erhel, S., Jamet, É. & Rouxel, G. (2015). What links between user experience and acceptability? In ACM (Hg.), *Proceedings of the 27th Conference on l'Interaction Homme-Machine* (S. 1–6). ACM. https://doi.org/10.1145/2820619.2825015

Martínez-Torres, M. R., Díaz-Fernández, M. C., Toral, S. L. & Barrero, F. J. (2013). Identification of new added value services on intelligent transportation systems. *Behaviour & Information Technology*, *32*(3), 307–320. https://doi.org/10.1080/0144929X.2010.529942

Masur, P. K., Teutsch, D. & Trepte, S. (2017). Entwicklung und Validierung der Online-Privatheitskompetenzskala (OPLIS). *Diagnostica*, *63*(4), 256–268. https://doi.org/10.1026/0012-1924/a000179

Mayer, R. C., Davis, J. H. & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of management review*, *20*(3), 709–734.

McAuley, D., Mortier, R. & Goulding, J. (2011). The Dataware manifesto. In *Third International Conference on Communication Systems and Networks (COMSNETS), 2011: 4 - 8 Jan. 2011, Bangalore, India ; [including workshop papers* (S. 1–6). IEEE. https://doi.org/10.1109/COMSNETS.2011.5716491

Milne, G. R., Pettinico, G., Hajjat, F. M. & Markos, E. (2017). Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. *Journal of Consumer Affairs*, *51*(1), 133–161. https://doi.org/10.1111/joca.12111

Mishra, D., Akman, I. & Mishra, A. (2014). Theory of Reasoned Action application for Green Information Technology acceptance. *Computers in Human Behavior*, *36*, 29–40. https://doi.org/10.1016/j.chb.2014.03.030

Mital, M., Chang, V., Choudhary, P., Papa, A. & Pani, A. K. (2018). Adoption of Internet of Things in India: A test of competing models using a structured equation modeling approach. *Technological Forecasting and Social Change*, *136*, 339–346. https://doi.org/10.1016/j.techfore.2017.03.001

Molm, L. D., Takahashi, N. & Peterson, G. (2000). Risk and Trust in Social Exchange: An Experimental Test of a Classical Proposition. *American Journal of Sociology*, *105*(5), 1396–1427.

Moons, I. & Pelsmacker, P. de (2012). Emotions as determinants of electric car usage intention. *Journal of Marketing Management*, *Vol. 28*(3-4), 196–237.

Moons, I. & Pelsmacker, P. de (2015). An Extended Decomposed Theory of Planned Behaviour to Predict the Usage Intention of the Electric Car: A Multi-Group Comparison. *Sustainability*, *7*(5), 6212–6245. https://doi.org/10.3390/su7056212

Moták, L., Neuville, E., Chambres, P., Marmoiton, F., Monéger, F., Coutarel, F. & Izaute, M. (2017). Antecedent variables of intentions to use an autonomous shuttle: Moving beyond TAM and TPB? *Revue Européenne de Psychologie Appliquée/European Review of Applied Psychology*, *67*(5), 269–278. https://doi.org/10.1016/j.erap.2017.06.001

Müller-Seitz, G., Dautzenberg, K., Creusen, U. & Stromereder, C. (2009). Customer acceptance of RFID technology: Evidence from the German electronic retail sector. *Journal of Retailing and Consumer Services*, *16*(1), 31–39. https://doi.org/10.1016/j.jretconser.2008.08.002

Myktytyn, P. P. & Harrison, D. A. (1993). The Application of the Theory of Reasoned Action to Senior Management and Strategic Information Systems. *Information Resources Management Journal*, *6*(2), 15–26.

Naab, K. (2004). Sensorik- und Signalverarbeitungsarchitekturen für Fahrerassistenz und Aktive Sicherheit. In M. Lienkamp (Vorsitz), *1. Tagung Aktive Sicherheit durch Fahrerassistenzsysteme.* Symposium im Rahmen der Tagung von TU München, München.

Nadal, C., Sas, C. & Doherty, G. (2019). Technology acceptability, acceptance and adoption - definitions and measurement. In N. Weibel & K. Unertl (Vorsitz), *Symposium: Workgroup on Interactive Systems in Health 2019 (WISH '19),* Glasgow, UK.

Nor, K. M., Abu Shanab, E. A. & Pearson, J. M. (2008). Internet Bankging Acceptance in Malaysia Based on the Theory of Reasoned Action. *Journal of Information Systems and Technology Management*, *5*(1), 3–14.

Nysveen, H. & Pedersen, P. E. (2016). Consumer adoption of RFID-enabled services. Applying an extended UTAUT model. *Information Systems Frontiers*, *18*(2), 293–314. https://doi.org/10.1007/s10796-014-9531-4

Oltramari, A., Piraviperumal, D., Schaub, F., Wilson, S., Cherivirala, S., Norton, T. B., Russell, N. C., Story, P., Reidenberg, J. & Sadeh, N. (2018). PrivOnto: A Semantic Framework for the Analysis of Privacy Policies. *Semantic Web*, *9*(2), 185–203.

Oreg, S. & Katz-Gerro, T. (2006). Predicting Proenvironmental Behavior Cross-Nationally. *Environment and Behavior*, *38*(4), 462–483. https://doi.org/10.1177/0013916505286012

Osswald, S., Wurhofer, D., Trösterer, S., Beck, E. & Tscheligi, M. (2012). Predicting Information Technology Usage in the Car: Towards a Car Technology Acceptance Model. In A. L. Kun (Hg.), *Proceedings of the 4th International Conference on Automotive User Interfaces and Interactive Vehicular Applications* (S. 1–8). ACM.

Owens, J. M., Antin, J. F., Doerzaph, Z. & Willis, S. (2015). Cross-generational acceptance of and interest in advanced vehicle technologies: A nationwide survey. *Transportation Research Part F: Traffic Psychology and Behaviour*, *35*, 139–151. https://doi.org/10.1016/j.trf.2015.10.020

Park, E., Kim, H. & Ohm, J. Y. (2015). Understanding driver adoption of car navigation systems using the extended technology acceptance model. *Behaviour & Information Technology*, *34*(7), 741–751.

Park, E. (2020). User acceptance of smart wearable devices: An expectation-confirmation model approach. *Telematics and Informatics*, *47*, 101318. https://doi.org/10.1016/j.tele.2019.101318

Park, J., Kim, J., Nam, C. & Kim, S. (2013). Driver's intention to use smartphone-car connectivity. In International Telecommunications Society (Vorsitz), *24th European Regional Conference of the International Telecommunication Society,* Florence, Italy.

Pavlou, P. A. (2003). Consumer Acceptance of Electronic Commerce: Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model. *International Journal of Electronic Commerce*, *7*(3), 69–103.

Pavlou, P. A. & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior. *MIS Quarterly*, *30*(1), 115–143.

Payre, W., Cestac, J. & Delhomme, P. (2014). Intention to use a fully automated car: Attitudes and a priori acceptability. *Transportation Research Part F: Traffic Psychology and Behaviour*, *27*, 252–263.

Pelteret, M. & Ophoff, J. (2016). A Review of Information Privacy and Its Importance to Consumers and Organizations. *the international journal of an emerging transdiscipline*, *19*, 277–301.

Peslak, A., Ceccucci, W. & Sendall, P. (2012). An Empircial Study of Social Networking Behavior Using Theory of Reasoned Action. *Journal of Information Systems Applied Research*, *5*(3), 12–23.

Petschnig, M., Heidenreich, S. & Spieth, P. (2014). Innovative alternatives take action – Investigating determinants of alternative fuel vehicle adoption. *Transportation Research Part A: Policy and Practice*, *61*, 68–83. https://doi.org/10.1016/j.tra.2014.01.001

Plappert, C., Zelle, D., Krauß, C., Lange, B., Mauthöfer, S., Walter, J., Abendroth, B., Robrahn, R., Pape, T. von & & Decke, H. (2017). A Privacy-aware Data Access System for Automotive Applications. In *15th ESCAR Embedded Security in Cars Conference.*

Proust, J. (2012). The norms of acceptance. *Philosophical Issues*, *22*, 316–333.

Rahimi, B., Nadri, H., Lotfnezhad Afshar, H. & Timpka, T. (2018). A Systematic Review of the Technology Acceptance Model in Health Informatics. *Applied clinical informatics*, *9*(3), 604–634. https://doi.org/10.1055/s-0038-1668091

Read, W., Robertson, N. & McQuilken, L. (2011). A novel romance: The Technology Acceptance Model with emotional attachment. *Australian Marketing Journal (AMJ)*, *19*(4), 223–229. https://doi.org/10.1016/j.ausmj.2011.07.004

Reichwald, R., Meier, R. & Fremuth, N. (2002). Die mobile Ökonomie — Definition und Spezifika. In R. Reichwald (Hg.), *Mobile Kommunikation* (S. 3–16). Gabler Verlag.

Renaud, K. & van Blijon, J. (2008). Predicting Technology Acceptance and Adoption by the Elderly: A Qualitative study. In R. Botha (Hg.), *Proceedings of the 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries riding the wave of technology* (S. 210–219). ACM.

Rigdon, E. E., Sarstedt, M. & Ringle, C. M. (2017). On Comparing Results from CB-SEM and PLS-SEM: Five Perspectives and Five Recommendations. *Marketing ZFP*, *39*(3), 4–16. https://doi.org/10.15358/0344-1369-2017-3-4

SmartPLS 3 [Computer software]. (2015). SmartPLS GmbH. Boenningstedt.

Rohunen, A. & Markkula, J. (2018). On the road – listening to data subjects' personal mobility data privacy concerns. *Behaviour & Information Technology*, *281*, 1–17. https://doi.org/10.1080/0144929X.2018.1540658

Rokhiim, R., Wulandari, P. & Mayasari, I. (2018). Small medium enterprises Technology Acceptance Model: A conceptual review. *International Journal of Business and Society*, *19*(4), 686–699.

Roßnagel, A. (2015). Grundrechtsausgleich beim vernetzten Automobil. *Datenschutz und Datensicherheit*(6), 353–358.

Sahebi, S. & Nassiri, H. (2017). Assessing Public Acceptance of Connected Vehicle Systems in a New Scheme of Usage-Based Insurance. *Transportation Research Record: Journal of the Transportation Research Board*, *2625*(1), 62–69. https://doi.org/10.3141/2625-07

Sarver, V. T. (1983). Ajzen and Fishbein's "theory of reasoned action": A critical assessment. *Journal for the Theory of Social Behaviour*, *13*(2), 155–163.

Sathyendra, K. M., Ravichander, A., Story, P. G., Black, A. W. & Sadeh, N. (December 2017). *Helping Users Understand Privacy Notices with Automated Query Answering Functionality: An Exploratory Study* (CMU-ISR-17-114R). Pitsburgh, Pennsylvania. School of Computer Science, Carnegie Mellon University.

Scherer, R., Siddiq, F. & Tondeur, J. (2019). The technology acceptance model (TAM): A meta-analytic structural equation modeling approach to explaining teachers' adoption of digital technology in education. *Computers & Education*, *128*, 13–35. https://doi.org/10.1016/j.compedu.2018.09.009

Schmidt, T., Philipsen, R., Themann, P. & Ziefle, M. (2016). Public Perception of V2X-Technology – Evaluation of General Advantages, Disadvantages and Reasons for Data Sharing with

Connected Vehicles. In IEEE Intelligent Transportation Systems Society (Hg.), *2016 IEEE Intelligent Vehicles Symposium (IV)* (S. 1344–1349). IEEE.

Schmidt, T., Philipsen, R. & Ziefle, M. (2017). Dos and Don'ts of Datasharing in V2X-Technology. In M. Helfert, C. Klein, B. Donnellan & O. Gusikhin (Hg.), *Communications in Computer and Information Science: Bd. 738. Smart Cities, Green Technologies, and Intelligent Transport Systems: 5th International Conference, SMARTGREENS 2016, and Second International Conference, VEHITS 2016, Rome, Italy, April 23-25, 2016, Revised Selected Papers* (Bd. 738, S. 257–274). Springer International Publishing; Imprint; Springer. https://doi.org/10.1007/978-3-319-63712-9_15

Schoettle, B. & Sivak, M. (2014). *A survey of public opinion about connected vehicles in the U.S., the U.K., and Australia.*

Sheller, M. (2004). Automotive Emotions. *Theory, Culture & Society*, *21*(4-5), 221–242. https://doi.org/10.1177/0263276404046068

Shevchuk, N., Benson, V. & Oinas-Kukkonen, H. (2019). Risk and Self-Disclosure in Sustainable Persuasive Smart Home Technologies. In G. Rodriguez-Abitia & C. Ferran (Vorsitz), *Twenty-fifth Americas Conference on Information Systems 2019*. Symposium im Rahmen der Tagung von Association for Information Systems, Cancun.

Shin, J., Bhat, C. R., You, D., Garikapati, V. M. & Pendyala, R. M. (2015). Consumer preferences and willingness to pay for advanced vehicle technology options and fuel types. *Transportation Research Part C: Emerging Technologies*, *60*, 511–524.

Shoemaker, D. W. (2010). Self-exposure and exposure of the self: informational privacy and the presentation of identity. *Ethics and Information Technology*, *12*(1), 3–15. https://doi.org/10.1007/s10676-009-9186-x

Siegel, J. E., Erb, D. C. & Sarma, S. E. (2018). A Survey of the Connected Vehicle Landscape—Architectures, Enabling Technologies, Applications, and Development Areas. *IEEE Transactions on Intelligent Transportation Systems*, *19*(8), 2391–2406. https://doi.org/10.1109/TITS.2017.2749459

Simon, T. R., Guhr, N. & Breitner, M. H. (2013). *User Acceptance of Mobile Services to Support and Enable Car Sharing: A First Empirical Study*. Hannover. Universität Hannover.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly*, *35*(4), 989–1016.

Sommer, E. (2018). *Erfassung der Gebrauchstauglichkeit einer fahrzeugbezogenen Datenschutzapplikation* [Studienarbeit]. Technische Universität Darmstadt, Darmstadt.

Sonneberg, M.-O., Werth, O., Leyerer, M., Wille, W., Jarlik, M. & Breitner, M. H. (2019). An Empirical Study of Customers' Behavioral Intention to Use Ridepooling Services – An Extension of the Technology Acceptance Model. In T. Ludwig, V. Pipek & G. Stevens (Vorsitz), *14th International Conference on Wirtschaftsinformatik,* Siegen.

Spaar, D. (2016). Daten auf Rädern: Was moderne Autos speichern und wie man an die Informationen herankommt. *c't,* 2016(9/2016), S. 170–172.

Spinello, R. (2015). The Right to Privacy in the Age of Digital Technology. In M. Badra & S. Zeadally (Hg.), *Computer Communications and Networks. Privacy in a digital, networked world: Technologies, implications and solutions* (Bd. 89, S. 291–312). Springer. https://doi.org/10.1007/978-3-319-08470-1_13

Statista. (2018). *Prognostizierte Anzahl an vernetzten Fahrzeugen im Connected Car Markt in Deutschland von 2017 bis 2023 nach Subsegmenten*. https://de.statista.com/statistik/daten/studie/893909/umfrage/connected-car-anzahl-der-fahrzeuge-in-deutschland/

Statista. (2019a). *Anzahl der Smartphone-Nutzer in Deutschland in den Jahren 2009 bis 2018 (in Millionen)*. https://de.statista.com/statistik/daten/studie/198959/umfrage/anzahl-der-smartphonenutzer-in-deutschland-seit-2010/

Statista. (2019b). *Connected car worldwide*. https://www.statista.com/outlook/320/100/connected-car/worldwide

Steg, L. (2005). Car use: lust and must. Instrumental, symbolic and affective motives for car use. *Transportation Research Part A: Policy and Practice*, *39*(2-3), 147–162. https://doi.org/10.1016/j.tra.2004.07.001

Strickland, L. H., Lewicki, R. J. & Katz, A. M. (1966). Temporal Orientation and Perceived Control as Determinants of Risk-Taking. *Journal of Experimental Social Psychology*(2), 143–151.

Sung, J. & Jo, J. (2018). The influence of perceived risk and consumer innovativeness on intention to use of internet of things service. *Journal of theoretical and applied information technology*, *96*(4), 1008–1017.

Svangren, M. K., Skov, M. B. & Kjeldskov, J. (2017). The connected car. In Y. Rogers & A. S. I. G. o. C.-H.M. Interaction (Hg.), *Proceedings of the 19th International Conference on Human-Computer Interaction with Mobile Devices and Services* (S. 1–12). ACM. https://doi.org/10.1145/3098279.3098535

Tavani, H. T. (2008). Informational Privacy: Concepts, Theories, and Controversies. In K. E. Himma & H. T. Tavani (Hg.), *Handbook of Information and Computer Ethics* (S. 131–164). John Wiley & Sons.

Tavani, H. T. & Moor, J. H. (2001). Privacy protection, control of information, and privacy-enhancing technologies. *ACM Sigcas Computers in Society*, *31*(3), 6–11.

Tene, O. & Polonetsky, J. (2013, April). Big Data for All: Privacy and User Control in the Age of Analytics, 240–273.

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhöfer, A. & Lind, F. (2015). Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In S. Gutwirth, R. Leenes & P. de Hert (Hg.), *Reforming European Data Protection Law* (S. 333–365). Springer Netherlands. https://doi.org/10.1007/978-94-017-9385-8_14

Tsai, J. Y., Egelman, S., Cranor, L. & Acquisti, A. (2011). The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, *22*(2), 254–268. https://doi.org/10.1287/isre.1090.0260

Tucker, C. E. (2014). Social Networks, Personalized Advertising, and Privacy Controls. *Journal of marketing research*, *51*(5), 546–562.

Ussat, M. A. C. (2012). *Personalisierte Optionsauswahl im Fahrzeuginformationssystem: Evaluierung verschiedener Assistenzarten im fahrzeugspezifischen Nutzungskontext* [Dissertation]. Humbolt Universität zu Berlin, Berlin.

Vallerand, R. J., Deshaies, P., Cuerrier, J.-P., Pelletier, L. G. & Mongeau, C. (1992). Ajzen and Fishbein's Theory of Rasoned Action as Applied to Moral Behavior: A Confirmatory Analysis. *Personality processes and individual differences*, *62*(1), 98–109.

van der Heijden, H. (2003). Factors influencing the usage of websites: the case of a generic portal in The Netherlands. *Information & Management*, *40*(6), 541–549. https://doi.org/10.1016/S0378-7206(02)00079-4

Venkatesh, V. & Bala, H. (2008). Technology Acceptance Model 3 and a Research Agenda on Interventions, *Vol. 39*(No. 2), 273–315.

Venkatesh, V. & Davis, F. D. (2000). A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies, *Vol. 46*(No. 2), 186–204.

Venkatesh, V., Morris, M. G., Davis, G. B. & Davis, F. D. (2003). User Acceptance of information technology: Toward a unified view. *MIS Quarterly*, *47*(3), 425–478.

Verband der Automobilindustrie. (2014). *Datenschutz-Prinzipien für vernetzte Fahrzeuge*. Berlin. Verband der Automobilindustrie e.V.

Vetter, J. (2018). *Erhebung und Analyse von Blickbewegungen bei der Nutzung einer fahrzeugbasierten Datenschutzapplikation* [Bachelorthesis]. Technische Universität Darmstadt, Darmstadt.

Vogt, J., Wieker, H. & Fuenfrocken, M. (2015). Architektur fuer die vernetzte Verkehrszukunft. Der ITS-Systemverbund Converge. *Internationales Verkehrswesen*, 66–74.

Wachter, S. (2018). Ethical and normative challenges of identification in the Internet of Things. In IET (Vorsitz), *Living in the Internet of Things: Cybersecurity of the IoT - 2018,* London.

Walsh, S. P., White, K. M., Hyde, M. K. & Watson, B. (2008). Dialling and Driving: Factors Influencing Intentions to Use a Mobile Phone While Driving., 1–37.

Walter, J., Abendroth, B., Pape, T. von, Plappert, C., Zelle, D., Krauß, C., Gagzow, G. & Decke, H. (2018). The user-centered privacy-aware control system PRICON. In ACM (Hg.), *ARES 2018: 13th International Conference on Availability, Reliability and Security : August 27 - August 30, 2018, University of Hamburg, Hamburg, Germany* (S. 1–10). Association for Computing Machinery. https://doi.org/10.1145/3230833.3233269

Walter, J. & Abendroth, B. (2018). Losing a Private Sphere? A Glance on the User Perspective on Privacy in Connected Cars. In C. Zachäus, B. Müller & G. Meyer (Hg.), *Lecture Notes in Mobility. Advanced microsystems for automotive applications 2017: Smart systems transforming the automobile* (Bd. 223, S. 237–247). Springer. https://doi.org/10.1007/978-3-319-66972-4_20

Walter, J., Abendroth, B. & Agarwal, N. (2017). PRICON: Selft-determined privacy in the connecte car motivated by the privacy calculus model. In J. Williamson & S. Schneegass (Hg.), *ICPS, MUM 2017: 16th International Conference on Mobile and Ubiquitous Multimedia : proceedings : Nov 26 - Nov 29, 2017, Stuttgart, Germany* (S. 421–427). The Association for Computing Machinery Inc. https://doi.org/10.1145/3152832.3156627

Walter, J., Birgmeier, M. & Abendroth, B. (2020). Entwicklung eines kombinierten Klassifikationssystems für vernetzte Mehrwertdienste und Fahrerassistenzsysteme im Automobil. In Gesellschaft für Arbeitswissenschaft (Hg.), *Tagungsband des 66. Frühjahrskongresses der Gesellschaft für Arbeitswissenschaft e.V. 2020: Digitaler Wandel, digitale Arbeit, digitaler Mensch?*.

Wang, E. S.-T. & Lin, R.-L. (2016). Perceived quality factors of location-based apps on trust, perceived privacy risk, and continuous usage intention. *Behaviour & Information Technology*, *12*(2), 1–9. https://doi.org/10.1080/0144929X.2016.1143033

Wang, J., Amos, B., Das, A., Pillai, P., Sadeh, N. & Satyanarayanan, M. (2017). A Scalable and Privacy-Aware IoT Service for Live Video Analytics. In Unknown (Hg.), *Proceedings of the 8th*

ACM Multimedia Systems Conference, MMSys'17: Taipei, Taiwan, June 20 - 23, 2017 (S. 38–49). ACM. https://doi.org/10.1145/3083187.3083192

Wardak, W. (2017). *Konzeption einer szenario-basierten Wizard-of-Oz Simulation für den Fahrsimulator* [Studienarbeit]. Technische Universität Darmstadt, Darmstadt.

Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Havard Law Review*, *4*(5), 193–220.

Weber, H., Krings, J., Seyfferth, J., Güthner, H. & Neuhausen, J. (2019). *Digital Auto Report 2019*. PWC Strategy&.

Welling, A. (2019). *Intelligent und sicher - aber auch akzeptiert? Entwicklung und Umsetzung eines animierten Videos zur Visualisierung eines vernetzten Mehrwertdienstes im Fahrzeug* [Bachelorthesis]. Technische Universität Darmstadt, Darmstadt.

Westin, A. F. (1967). *Privacy and Freedom*. Atheneum.

Westin, A. F. (2003). Social and Political Dimensions of Privacy. *Journal of Social Issues*, *59*(2), 431–453.

Williams, M. D., Rana, N. P. & Dwivedi, Y. K. (2015). The unified theory of acceptance and use of technology (UTAUT): a literature review. *Journal of Enterprise Information Management*, *28*(3), 443–488. https://doi.org/10.1108/JEIM-09-2014-0088

Wilson, D. W., Schuetzler, R. M., Dorn, B. & Proudfoot, J. G. (2015). When Disclosure is Involuntary: Empowering Users with Control to Reduce Concerns. *Information Systems and Quantitative Analysis Faculty Proceedings & Presentations*, *17*.

Winkelhake, U. (2017). *Die digitale Transformation der Automobilindustrie: Treiber - Roadmap - Praxis*. Springer Vieweg.

Winner, H., Hakuli, S., Lotz, F. & Singer, C. (Hg.). (2015). *Handbuch Fahrerassistenzsysteme: Grundlagen, Komponenten und Systeme für aktive Sicherheit und Komfort* (3. Aufl.). Springer Fachmedien Wiesbaden.

Wirtz, B. W. & Göttel, V. (2016). Technology Acceptance in social media: Review, synthesis and directions for future empirical research. *Journal of Electronic Commerce Research*, *17*(2), 97–115.

Wittler, M. (24. Juni 2020). Autokauf ohne Anfassen: Online zum Neuwagen. *Spiegel*. https://www.spiegel.de/auto/auto-kaufen-im-internet-audi-mercedes-opel-und-co-auf-neuen-wegen-a-82cd536e-3795-46a8-a48f-fa4758166b0d

Wong, K. K.-K. (2013). Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS. *Marketing Bulletin*, *24*, Artikel Technical Note 1, 1–32.

Wu, J., Liao, H., Wang, J.-W. & Chen, T. (2019). The role of environmental concern in the public acceptance of autonomous electric vehicles: A survey from China. *Transportation Research Part F: Traffic Psychology and Behaviour*, *60*, 37–46. https://doi.org/10.1016/j.trf.2018.09.029

Xu, F., Michael, K. & Chen, X. (2013). Factors affecting privacy disclosure on social network sites: an integrated model. *Electronic Commerce Research*, *13*(2), 151–168. https://doi.org/10.1007/s10660-013-9111-6

Xu, H., Dinev, T., Smith, J. & Hart, P. (2011). Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems (JAIS)*, *12*(12), 798–824.

Xu, H. & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets*, *19*(2-3), 137–149. https://doi.org/10.1007/s12525-009-0012-4

Xu, H., Teo, H.-H., Tan, B. C. Y. & Agarwal, R. (2009). The Role of Push-Pull Technology in Privacy Calculus: The Case of Location-Based Services. *Journal of Management Information Systems*, *26*(3), 135–174. https://doi.org/10.2753/MIS0742-1222260305

Yang, H., Lee, H. & Zo, H. (2017). User acceptance of smart home services: an extension of the theory of planned behavior. *Industrial Management & Data Systems*, *117*(1), 68–89. https://doi.org/10.1108/IMDS-01-2016-0017

Yang, S. & Wang, K. (2009). The Influence of Information Sensitivity The influence of information sensititvity compensation on privacy concern and behavioral intention. *The DATA BASE for Advances in Information Systems*, *40*(1), 38–51.

Yoon, S.-B. & Cho, E. (2016). Convergence adoption model (CAM) in the context of a smart car service. *Computers in Human Behavior*, *60*, 500–507. https://doi.org/10.1016/j.chb.2016.02.082

Zaunbrecher, B. S., Bexten, T., Wirsum, M. & Ziefle, M. (2016). What is Stored, Why, and How? Mental Models, Knowledge, and Public Acceptance of Hydrogen Storage. *Energy Procedia*, *99*, 108–119. https://doi.org/10.1016/j.egypro.2016.10.102

Zhang, Y., Li, J., Zheng, D., Li, P. & Tian, Y. (2018). Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice. *Journal of Network and Computer Applications*, *122*, 50–60. https://doi.org/10.1016/j.jnca.2018.07.017

Zhao, L., Lu, Y. & Gupta, S. (2012). Disclosure Intention of Location-Related Information in Location-Based Social Network Services. *International Journal of Electronic Commerce*, *16*(4), 53–90. https://doi.org/10.2753/JEC1086-4415160403

Zhou, T. (2012). Examining location-based services usage from the perspective of unified theory of acceptance and use of technology and privacy risk. *Journal of Electronic Commerce Research*, *13*(2), 135–144.

Zhu, L., Yu, F. R., Wang, Y., Ning, B. & Tang, T. (2019). Big Data Analytics in Intelligent Transportation Systems: A Survey. *IEEE Transactions on Intelligent Transportation Systems*, *20*(1), 383–398. https://doi.org/10.1109/TITS.2018.2815678

Zmud, J., Sener, I. N. & Wagner, J. (2016). *Consumer Acceptance and Travel Behavior Impacts of Automated Vehicles*. Austin. Texas A&M Transportation Institute.

Abbildungsverzeichnis

Tabellenverzeichnis

Anhang

Anhang 1: Interne Konsistenz der Skalen im Pretest

Tabelle A1. Übersicht über die interne Konsistenz der einzelnen Skalen nach dem Pretest (N = 33). *Kursiv* gedruckte Skalen erfüllen nicht das geforderte Mindestmaß an interner Konsistenz ($\alpha \geq 0.7$).

Skala	**N_{Items}**	**Cronbach's α (≥ .7)**
Wahrgenommene Nützlichkeit	*3*	*0,69*
Wahrgenommene Einfachheit der Nutzung	3	0,87
Einstellung gegenüber der Nutzung des Systems	*3*	*0,68*
Wahrgenommene Informationskontrolle	3	0,90
Privatheitsbedenken	3	0,86
Vertrauen in den Anbieter	3	0,88
Wahrgenommenes Privatheitsrisiko	*3*	*0,69*
Soziale Norm	3	0,86
Verhaltensintention	3	0,81

Anhang 2: Finaler Fragebogen für Studie 1

Tabelle A2. Finaler Fragebogen für Studie 1mit den Faktorladungen der einzelnen Items sowie den Qualitätskriterien der Skalen.

Skala/Item	Ladung	Cronbach's Alpha	Komposite Reliabilität	AVE
Einstellung gegenüber der Nutzung		0.772	0.869	0.688
Die Nutzung der Parkplatzapplikation während der Fahrt macht Spaß.	0.837			
Ich mag die Vorstellung, dass ich die Parkplatzapplikation nutze, nicht.	0.790			
Die Parkplatzapplikation macht die Autofahrt komfortabler.	0.860			
Nutzungsintention		0.877	0.924	0.803
Ich will die Parkplatzapplikation während der Fahrt gar nicht haben.	0.889			
Ich habe vor die Parkplatzapplikation so oft wie möglich während der Fahrt zu nutzen.	0.874			
Sofern es möglich ist, möchte ich die Parkplatzapplikation während der Fahrt nutzen.	0.924			
Wahrgenommene Nützlichkeit		0.833	0.889	0.668
Durch die Nutzung der Applikation spare ich Zeit.	0.848			
Die Nutzung der Parkplatzapplikation vereinfacht die Parkplatzsuche.	0.824			
Ich finde den Einsatz der Applikation während der Fahrt nicht nützlich.	0.854			
Die Vorteile der Parkplatzapplikation überwiegen die Nachteile.	0.739			

Wahrgenommene Einfachheit d. Nutzung		0.830	0.888	0.665
Das Erlernen der Bedienung der Parkplatzapplikation ist einfach.	0.781			
Es fällt mir leicht mit der Parkplatzapplikation umzugehen.	0.808			
Die Parkplatzapplikation ist einfach zu bedienen.	0.898			
Die Interaktion mit der Parkplatzapplikation ist klar und verständlich.	0.769			
Wahrgenommene Informationskontrolle		0.883	0.927	0.810
Ich glaube, dass ich die Kontrolle darüber habe, wer Zugang zu meinen persönlichen Informationen erhält.	0.895			
Ich glaube, dass ich die Kontrolle darüber habe, wie persönliche Informationen von der Parkplatzapplikation genutzt werden.	0.917			
Ich denke, dass ich die Kontrolle darüber habe, welche persönliche Informationen von der Parkplatzapplikation bereit gestellt werden.	0.888			
Privatheitsbedenken		0.925	0.952	0.870
Ich bin besorgt, dass die Informationen, die ich an die Parkplatzapplikation preisgebe, missbraucht werden könnten.	0.940			
Ich bin darüber besorgt, was andere mit den persönlichen Informationen machen könnten, die ich an die Parkplatzapplikation preisgegeben habe.	0.916			

Ich bin wegen der Datenpreisgabe an die Parkplatzapplikation besorgt, da meine Daten anders als von mir vorhergesehen genutzt werden könnten.	0.942			
Wahrgenommenes Privatheitsrisiko		0.907	0.942	0.843
Die Preisgabe meiner persönlichen Daten an die ConCar AG kann viele unerwartete Probleme bedingen.	0.936			
Es ist riskant meine persönlichen Daten an die ConCar AG preiszugeben.	0.913			
Es besteht eine große Gefahr, dass ich die Kontrolle über meine Daten durch die Preisgabe an die ConCar AG verliere.	0.905			
Vertrauen in den Anbieter		0.739	0.851	0.656
Der Anbieter der Parkplatzapplikation hat die Kundeninteressen im Blick.	0.777			
Der Anbieter der Parkplatzapplikation hält seine Versprechen.	0.758			
Der Anbieter der Parkplatzapplikation ist vertrauenswürdig.	0.890			
Soziale Norm		0.806	0.886	0.721
Ich wäre stolz die Parkplatzapplikation Personen zu zeigen, die mir Nahe stehen.	0.847			
Personen, deren Meinung mir wichtig ist, würden dieses System ebenfalls mögen.	0.825			
Meine Freunde würden mich bestärken, die Parkplatzapplikation zu benutzen.	0.875			

Anhang 3: Ergebnisse des Strukturgleichungsmodells ohne Informationskontrolle (Forschungsfrage 1) für die datenpreisgebenden Teilnehmenden

Tabelle A3. Ergebnisse der Neuberechnung des Strukturgleichungsmodells auf Basis der Teilnehmenden, die die angeforderten Daten im Zuge der Nutzung der ParkingApp preisgegeben haben (N = 103).

Hypothese	*Beziehung*	*β*	*t*	*p*	
H 1.1	PU → ATT	0,618	5,83	< .001	H_0 abgelehnt
H 1.2	PU → BI	0,02	0,14	> .05	H_0 nicht abgelehnt
H 1.3	PEOU → PU	0,50	4,01	< .001	H_0 abgelehnt
H 1.4	PEOU → ATT	-0,02	0,31	> .05	H_0 nicht abgelehnt
H 1.5	ATT → BI	0,50	5,82	< .001	H_0 abgelehnt
H 1.6	SN → BI	0,35	4,14	< .001	H_0 abgelehnt
H 1.7	PC → PR	0,78	18,86	< .001	H_0 abgelehnt
H 1.8	PC → TR	-0,31	3,41	< .001	H_0 abgelehnt
H 1.9	TR → BI	-0,03	0,47	> .05	H_0 nicht abgelehnt
H 1.10	TR → PR	-0,09	1,71	> .05	H_0 nicht abgelehnt
H 1.11	PR → BI	-0,13	2,06	< .05	H_0 abgelehnt
H 1.12	PR → ATT	-0,14	1,77	> .05	H_0 nicht abgelehnt
H 1.13	IC → PR	-0,09	1,35	> .05	H_0 nicht abgelehnt
H 1.14	IC → PC	-0,34	3,84	< .001	H_0 abgelehnt

Anhang 4: Strukturgleichungsmodell unter der Bedingung ohne tatsächlicher Informationskontrolle (nur datenpreisgebende Teilnehmende)

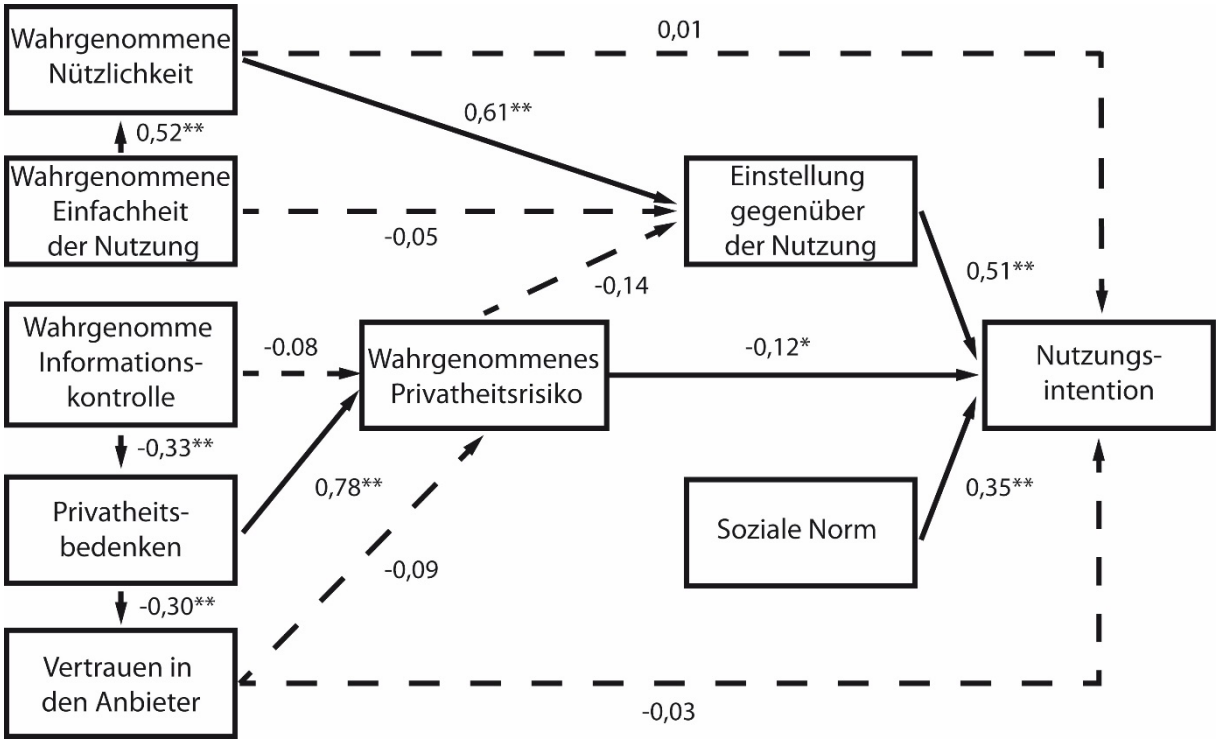


Abbildung A1. Strukturgleichungsmodell für die Nutzung des vernetzten Parkdienstes auf der Basis der Teilstichprobe der datenpreisgebenden Teilnehmenden (N = 103). Gestrichelte Linien kennzeichnen nicht-signifikante Pfadbeziehungen.

Anhang 5: Strukturgleichungsmodell unter der Bedingung mit tatsächlicher Informationskontrolle

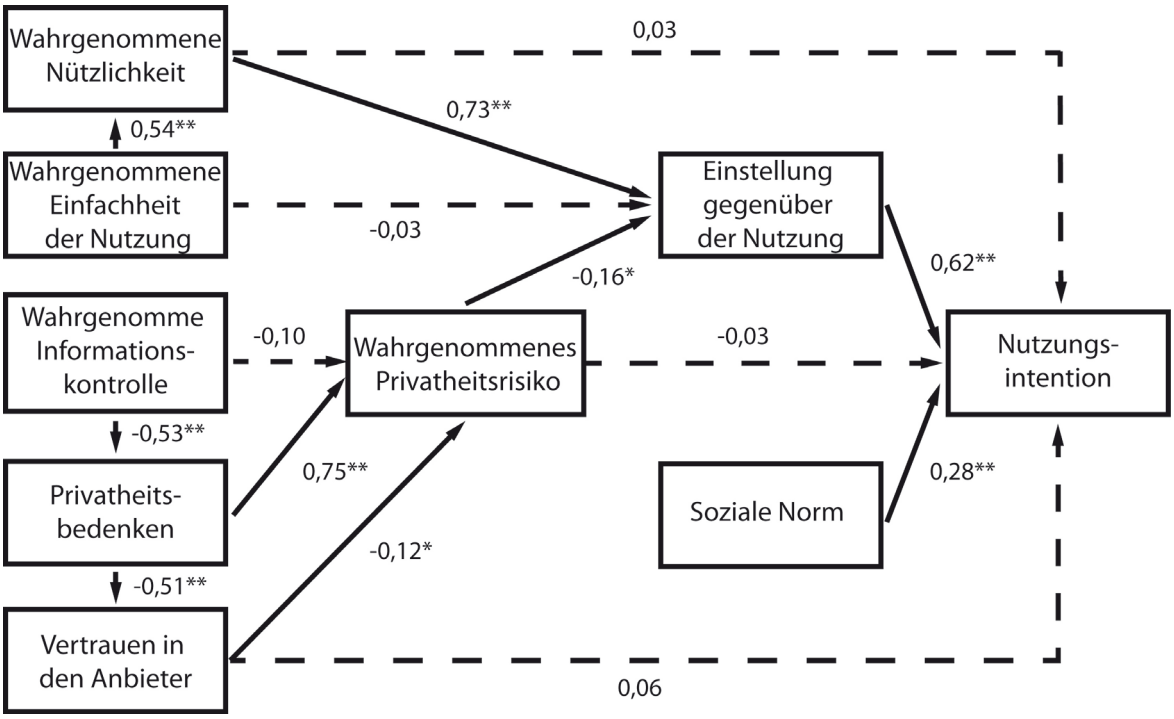


Abbildung A2. Strukturgleichungsmodell für die vernetzte Parkdienstnutzung unter dem Vorleigen einer tatsächlichen Informationskontrolle. Dargestellt werden die Pfadkoeffizienten β. Gestrichelte Pfade kennzeichnen nicht signifikante Pfadbeziehungen.

Anhang 6: Etablierung der Messinvarianz für Konstrukt-basierte Modelle (*measurement invariance of composite models (MICOM)*)

Tabelle A4. Ergebnisse des zweiten Schritts der Etablierung von MICOM: Sicherstellung der kompositionellen Invarianz. *Kursiv* gedruckte Konstrukte erfüllen die kompositionelle Invarianz nicht.

Konstrukte	**Korrelation *r* zwischen *pre* versus *post* PRICON**	***p***
Einstellung	0,998	> .1
Nutzungsintention	*0,997*	*< .05*
Privatheitsbedenken	1,000	> .5
Privatheitsrisiko	1,000	> .5
Nützlichkeit	1,000	> .5
Einfachheit der Nutzung	0,999	> .5
Informationskontrolle	1,000	> .5
Vertrauen in den Anbieter	0,998	> .5
Soziale Norm	1,000	> .5

Hinweis: Signifikanzniveau ist α = .05. Konstrukte mit p < .05 erfüllen die Bedingung der kompositionellen Invarianz nicht.

Anhang 7: Ergebnisse der PLS Multigruppenanalyse zwischen der Bedingung mit versus ohne Informationskontrolle

Tabelle A5. Ergebnisse des parametrischen Tests zur PLS-Multigruppenanalyse. Pfadbeziehungen, die die Nutzungsintention einschließen, sind nicht inkludiert, da die Nutzungsintention die Bedingung der kompositionellen Invarianz nicht erfüllt (siehe Tabelle A3).

	$\lvert \beta_{pre} - \beta_{post} \rvert$	T	p
Privatheitsbedenken – Privatheitsrisiko	0,04	0,58	> .5
Privatheitsbedenken – Vertrauen	0,17	1,61	> .1
Einfachheit der Nutzung – Einstellung	0,01	0,05	> .5
Einfachheit der Nutzung – Nützlichkeit	0,01	0,05	> .5
Nützlichkeit – Einstellung	0,12	1,04	> .1
Informationskontrolle – Privatheitsbedenken	0,22	1,85	.07
Informationskontrolle - Privatheitsrisiko	0,04	0,39	> .5
Privatheitsrisiko – Einstellung	0,02	0,15	> .5
Vertrauen - Privatheitsrisiko	0,05	0,70	> .1

Hinweis: Signifikanzniveau ist α = .05.

Anhang 8: Fragebogen für Studie 2

Tabelle A6. Fragebogen für Studie 2 mit den Faktorladungen der einzelnen Items sowie den Qualitätskriterien der Skalen. Der Fragebogen basiert auf dem Fragebogen zu Studie 1 (siehe Tabelle A2).

Skala/Item	**Ladung**	**Cronbach's Alpha**	**Komposite Reliabilität**	**AVE**
Einstellung gegenüber der Nutzung		0,824	0,895	0,740
Die Nutzung des vernetzten Dienstes während der Fahrt macht Spaß.	0,766			
Ich mag die Vorstellung, dass ich den vernetzten Dienst nutze, nicht.	0,913			
Der vernetzte Dienst macht die Autofahrt effizienter.	0,893			
Nutzungsintention		0,959	0,973	0,924
Ich will den vernetzten Dienst während der Fahrt gar nicht haben.	0,953			
Ich habe vor den vernetzten Dienst so oft wie möglich während der Fahrt zu nutzen.	0,961			
Sofern es möglich ist, möchte ich den vernetzten Dienst während der Fahrt nutzen.	0,969			
Wahrgenommene Nützlichkeit		0,846	0,896	0,685
Durch die Nutzung des vernetzten Dienstes spare ich Zeit.	0,877			
Die Nutzung des vernetzten Dienstes vereinfacht meine Autofahrt.	0,853			
Ich finde den Einsatz des vernetzten Dienstes während der Fahrt nicht nützlich.	0,713			
Die Vorteile des vernetzten Dienstes überwiegen die Nachteile.	0,857			

Wahrgenommene Einfachheit d. Nutzung		0,761	0,860	0,672
Das Erlernen der Bedienung des vernetzten Dienstes wäre einfach.	0,764			
Der vernetzte Dienst wäre einfach zu bedienen.	0,836			
Die Interaktion mit dem vernetzten Dienst wäre klar und verständlich.	0,849			
Wahrgenommene Informationskontrolle		0,870	0,920	0,794
Ich glaube, dass ich die Kontrolle darüber habe, wer Zugang zu meinen persönlichen Informationen erhält.	0,874			
Ich glaube, dass ich die Kontrolle darüber habe, wie persönliche Informationen von dem vernetzten Dienst genutzt werden.	0,935			
Ich denke, dass ich die Kontrolle darüber habe, welche persönliche Informationen von dem vernetzten Dienst bereit gestellt werden.	0,862			
Privatheitsbedenken		0,944	0,964	0,900
Ich bin besorgt, dass die Informationen, die ich an den vernetzten Dienst preisgebe, missbraucht werden könnten.	0,945			
Ich bin darüber besorgt, was andere mit den persönlichen Informationen machen könnten, die ich an den vernetzten Dienst preisgegeben habe.	0,965			
Ich bin wegen der Datenpreisgabe an den vernetzten Dienst besorgt, da meine Daten anders als von mir vorhergesehen genutzt werden könnten.	0,935			

Wahrgenommenes Privatheitsrisiko		0,928	0,954	0,874
Die Preisgabe meiner persönlichen Daten an den Anbieter kann viele unerwartete Probleme bedingen.	0,944			
Es ist riskant meine persönlichen Daten an den Anbieter preiszugeben.	0,932			
Es besteht eine große Gefahr, dass ich die Kontrolle über meine Daten durch die Preisgabe an den Anbieter verliere.	0,929			
Vertrauen in den Anbieter		0,769	0,878	0,706
Der Anbieter des vernetzten Dienstes hat die Kundeninteressen im Blick.	0,897			
Der Anbieter des vernetzten Dienstes hält seine Versprechen.	0,740			
Der Anbieter des vernetzten Dienstes ist vertrauenswürdig.	0,876			
Soziale Norm		0,854	0,911	0,774
Ich wäre stolz den vernetzten Dienst Personen zu zeigen, die mir Nahe stehen.	0,863			
Personen, deren Meinung mir wichtig ist, würden dieses System ebenfalls mögen.	0,883			
Meine Freunde würden mich bestärken, den vernetzten Dienst zu benutzen.	0,892			

Anhang 9: Fragebogen für Studie 3

Tabelle A7. Fragebogen für Studie 3 mit den Faktorladungen der einzelnen Items sowie den Qualitätskriterien der Skalen. Der Fragebogen basiert auf den Fragebögen zu Studie 1 und 2 (siehe Tabellen A2 und A6).

Skala/Item	Ladung	Cronbach's Alpha	Komposite Reliabilität	AVE
Einstellung gegenüber der Nutzung		0,785	0,875	0,701
Die Nutzung des vernetzten Dienstes während der Fahrt macht Spaß.	0,776			
Ich mag die Vorstellung nicht, dass ich den vernetzten Dienst nutze.	0,903			
Der vernetzte Dienst macht die Autofahrt sicherer.	0,827			
Nutzungsintention		0,942	0,963	0,896
Ich will den vernetzten Dienst während der Fahrt gar nicht haben.	0,934			
Ich habe vor den vernetzten Dienst so oft wie möglich während der Fahrt zu nutzen.	0,948			
Sofern es möglich ist, möchte ich den vernetzten Dienst während der Fahrt nutzen.	0,958			
Wahrgenommene Nützlichkeit		0,836	0,902	0,755
Ich finde den vernetzten Dienst nützlich.	0,931			
Ich finde den Einsatz des vernetzten Dienstes während der Fahrt nicht nützlich.	0,840			
Die Vorteile des vernetzten Dienstes überwiegen die Nachteile.	0,832			
Wahrgenommene Einfachheit d. Nutzung		0,818	0,888	0,726
Das Erlernen der Bedienung des vernetzten Dienstes wäre einfach.	0,842			
Der vernetzte Dienst wäre einfach zu bedienen.	0,864			

Die Interaktion mit dem vernetzten Dienst wäre klar und verständlich.	0,851			
Wahrgenommene Informationskontrolle		0,934	0,958	0,883
Ich glaube, dass ich die Kontrolle darüber habe, wer Zugang zu meinen persönlichen Informationen erhält.	0,941			
Ich glaube, dass ich die Kontrolle darüber habe, wie persönliche Informationen von dem vernetzten Dienst genutzt werden.	0,943			
Ich denke, dass ich die Kontrolle darüber habe, welche persönliche Informationen von dem vernetzten Dienst bereit gestellt werden.	0,934			
Privatheitsbedenken		0,935	0,959	0,885
Ich bin besorgt, dass die Informationen, die ich an den vernetzten Dienst preisgebe, missbraucht werden könnten.	0,939			
Ich bin darüber besorgt, was andere mit den persönlichen Informationen machen könnten, die ich an den vernetzten Dienst preisgegeben habe.	0,957			
Ich bin wegen der Datenpreisgabe an den vernetzten Dienst besorgt, da meine Daten anders als von mir vorhergesehen genutzt werden könnten.	0,926			
Wahrgenommenes Privatheitsrisiko		0,891	0,932	0,821
Die Preisgabe meiner persönlichen Daten an den Anbieter kann viele unerwartete Probleme bedingen.	0,921			
Es ist riskant meine persönlichen Daten an den Anbieter preiszugeben.	0,911			

Es besteht eine große Gefahr, dass ich die Kontrolle über meine Daten durch die Preisgabe an den Anbieter verliere.	0,885			
Vertrauen in den Anbieter		0,778	0,872	0,696
Der Anbieter des vernetzten Dienstes hat die Kundeninteressen im Blick.	0,731			
Der Anbieter des vernetzten Dienstes hält seine Versprechen.	0,886			
Der Anbieter des vernetzten Dienstes ist vertrauenswürdig.	0,877			
Soziale Norm		0,842	0,904	0,759
Ich wäre stolz den vernetzten Dienst Personen zu zeigen, die mir Nahe stehen.	0,874			
Personen, deren Meinung mir wichtig ist, würden dieses System ebenfalls mögen.	0,877			
Meine Freunde würden mich bestärken, den vernetzten Dienst zu benutzen.	0,863			
Wahrgenommene Nützlichkeit (unzureichende diskriminante Validität)[1]		0,881	0,918	0,738
Durch die Nutzung des vernetzten Dienstes wird die Fahrt sicherer.		0,868		
Die Nutzung des vernetzten Dienstes macht meine Autofahrt sicherer.		0,877		
Ich finde den Einsatz des vernetzten Dienstes während der Fahrt nicht nützlich.		0,896		
Die Vorteile des vernetzten Dienstes überwiegen die Nachteile.		0,792		

[1] Diese Skala für die wahrgenommene Nützlichkeit wurde für die Berechnung des Modells aufgrund der unzureichenden diskriminanten Validität (siehe Tabelle A8) nicht verwendet, wird hier der Vollständigkeit halber dennoch berichtet.

Anhang 10: Überprüfung der Invarianz des Messmodells (MICOM)

Tabelle A8: Test der kompositionellen Invarianz sowie der Gleichheit der Mittelwerte und Varianzen zwischen den beiden experimentellen Gruppen in Studie 3.

	Stufe 2		Stufe 3			
	R_{Mean}	P_R	$M_{Differenz\ M}$	P_{Mean}	$M_{Differenz\ \sigma 2}$	$P_{\sigma 2}$
ATT	0,999	>.1	0,000	>.5	0,004	>.1
BI	1,000	>.1	0,000	>.5	0,005	>.5
IC	1,000	>.1	-0,002	>.5	0,005	>.5
PC	1,000	>.5	-0,001	>.5	0,005	>.5
PEOU	0,995	>.5	-0,001	>.5	0,002	>.1
PR	1,000	>.1	0,000	>.5	0,002	>.1
PU	0,999	>.5	-0,001	>.1	0,004	>.5
SN	0,999	>.5	-0,002	>.5	0,005	>.1
TR	0,998	>.1	0,002	>.1	0,001	>.5

Hinweis: Alle Werte basieren auf Permutationen mit N = 5000 Stichproben.

Anhang 11: Verletzung des Fornell-Larcker-Kriteriums

Tabelle A9. Cross-Ladungen und durchschnittlich erfasste Varianzen (AVEs) für Studie 3 mit den in Studie 2 verwendeten Items für PU. Die diskriminante Validität von ATT in Bezug zu PU ist unzureichend.

	ATT	BI	PU	PEOU	IC	PC	PR	TR	SN
ATT	*0,837*								
BI	0,808	0,947							
PU	*0,853*	0,754	0,859						
PEOU	0,476	0,418	0,528	0,852					
IC	0,564	0,644	0,519	0,343	0,940				
PC	-0,505	-0,638	-0,468	-0,192	-0,631	0,941			
PR	-0,574	-0,644	-0,512	-0,230	-0,639	0,864	0,906		
TR	0,738	0,670	0,672	0,364	0,626	-0,543	-0,589	0,834	
SN	0,700	0,752	0,619	0,238	0,589	-0,597	-0,573	0,663	0,871

Hinweis: Die AVEs sind auf der Diagonalen abgetragen. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Anhang 12: Cross-Ladungen für das ursprüngliche Messmodell in Studie 3

Tabelle A10. Cross-Ladungen für alle in den Studien 1-3 verwendeten Items für PU auf Basis der Daten aus Studie 3.

	ATT	BI	IC	PC	PEOU	PR	PU	SN	TR
ATT_1	*0,766*	0,659	0,517	-0,461	0,297	-0,484	0,575	0,625	0,552
ATT_2	*0,901*	0,781	0,499	-0,485	0,456	-0,551	0,771	0,649	0,704
ATT_4	*0,838*	0,579	0,406	-0,321	0,432	-0,402	0,786	0,484	0,586
BI_1	0,730	*0,934*	0,565	-0,582	0,358	-0,587	0,704	0,668	0,585
BI_2	0,780	*0,948*	0,631	-0,607	0,415	-0,608	0,713	0,748	0,655
BI_3	0,783	*0,958*	0,632	-0,623	0,412	-0,632	0,724	0,717	0,660
IC_1	0,495	0,563	0,941	-0,540	0,260	-0,553	0,438	0,515	0,566
IC_2	0,533	0,598	0,943	-0,584	0,355	-0,600	0,492	0,539	0,602
IC_3	0,558	0,647	0,934	-0,646	0,346	-0,641	0,527	0,598	0,592
PC_1	-0,539	-0,646	-0,609	0,939	-0,219	0,836	-0,507	-0,583	-0,568
PC_2	-0,448	-0,604	-0,586	0,957	-0,154	0,811	-0,436	-0,570	-0,487
PC_3	-0,436	-0,548	-0,586	0,926	-0,167	0,791	-0,374	-0,530	-0,476
PEOU_1	0,284	0,270	0,193	-0,050	0,838	-0,069	0,340	0,130	0,245
PEOU_3	0,366	0,318	0,252	-0,128	0,862	-0,128	0,424	0,157	0,298
PEOU_4	0,509	0,437	0,384	-0,259	0,855	-0,323	0,538	0,282	0,359
PR_1	-0,552	-0,612	-0,611	0,795	-0,226	0,921	-0,489	-0,521	-0,546
PR_2	-0,554	-0,618	-0,569	0,783	-0,249	0,911	-0,498	-0,531	-0,558
PR_3	-0,448	-0,513	-0,555	0,771	-0,143	0,885	-0,399	-0,505	-0,493
PU_1	0,718	0,543	0,425	-0,360	0,443	-0,391	0,868	0,481	0,562
PU_2	0,752	0,571	0,418	-0,338	0,444	-0,389	0,877	0,483	0,571
PU_3	0,805	0,770	0,465	-0,450	0,502	-0,479	0,896	0,599	0,593

PU_6	0,648	0,684	0,474	-0,454	0,420	-0,496	0,792	0,554	0,583
SN_1	0,668	0,721	0,541	-0,566	0,231	-0,528	0,590	0,874	0,593
SN_2	0,579	0,626	0,493	-0,484	0,195	-0,485	0,509	0,877	0,565
SN_3	0,574	0,607	0,501	-0,503	0,194	-0,481	0,512	0,863	0,574
Trust_1	0,567	0,514	0,460	-0,407	0,253	-0,432	0,522	0,470	0,731
Trust_2	0,628	0,561	0,540	-0,495	0,334	-0,535	0,582	0,591	0,886
Trust_3	0,649	0,600	0,561	-0,455	0,319	-0,501	0,577	0,591	0,877

Hinweis: Ladungen auf das intendierte Konstrukt sind unterstrichen. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Anhang 13: Ergebnisse aus Studie 3 mit ursprünglicher Skala für die wahrgenommene Nützlichkeit

Tabelle A11. Ergebnisse der Prüfung der Hypothesen zu Forschungsfrage 1 aus Studie 3 (Skala für wahrgenommene Nützlichkeit wie in Studien 1 und 2)

Hypothese	*Beziehung*	*β*	*t*	*p*	
H 1.1	PU → ATT	0,734	17,21	<.001	H_0 abgelehnt
H 1.2	PU → BI	0,20	2,69	<.01	H_0 abgelehnt
H 1.3	PEOU → PU	0,53	8,26	<.001	H_0 abgelehnt
H 1.4	PEOU → ATT	0,05	0,98	>.05	H_0 nicht abgelehnt
H 1.5	ATT → BI	0,34	3,54	<.001	H_0 abgelehnt
H 1.6	SN → BI	0,30	4,43	<.001	H_0 abgelehnt
H 1.7	PC → PR	0,73	15,55	<.001	H_0 abgelehnt
H 1.8	PC → TR	-0,55	11,04	<.001	H_0 abgelehnt
H 1.9	TR → BI	-0,02	0,37	>.05	H_0 nicht abgelehnt
H 1.10	TR → PR	-0,13	2,67	<.01	H_0 abgelehnt
H 1.11	PR → BI	-0,19	4,09	<.001	H_0 abgelehnt
H 1.12	PR → ATT	-0,19	4,68	<.001	H_0 abgelehnt
H 1.13	IC → PR	-0,10	1,710	>.05	H_0 nicht abgelehnt
H 1.14	IC → PC	-0,63	11,90	<.001	H_0 abgelehnt

Hinweis: Signifikanzniveau ist α = .05. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Anhang 14: Strukturgleichungsmodell für Studie 3 (sicherheitsbezogener Dienst) mit der ursprünglichen Skala für wahrgenommene Nützlichkeit

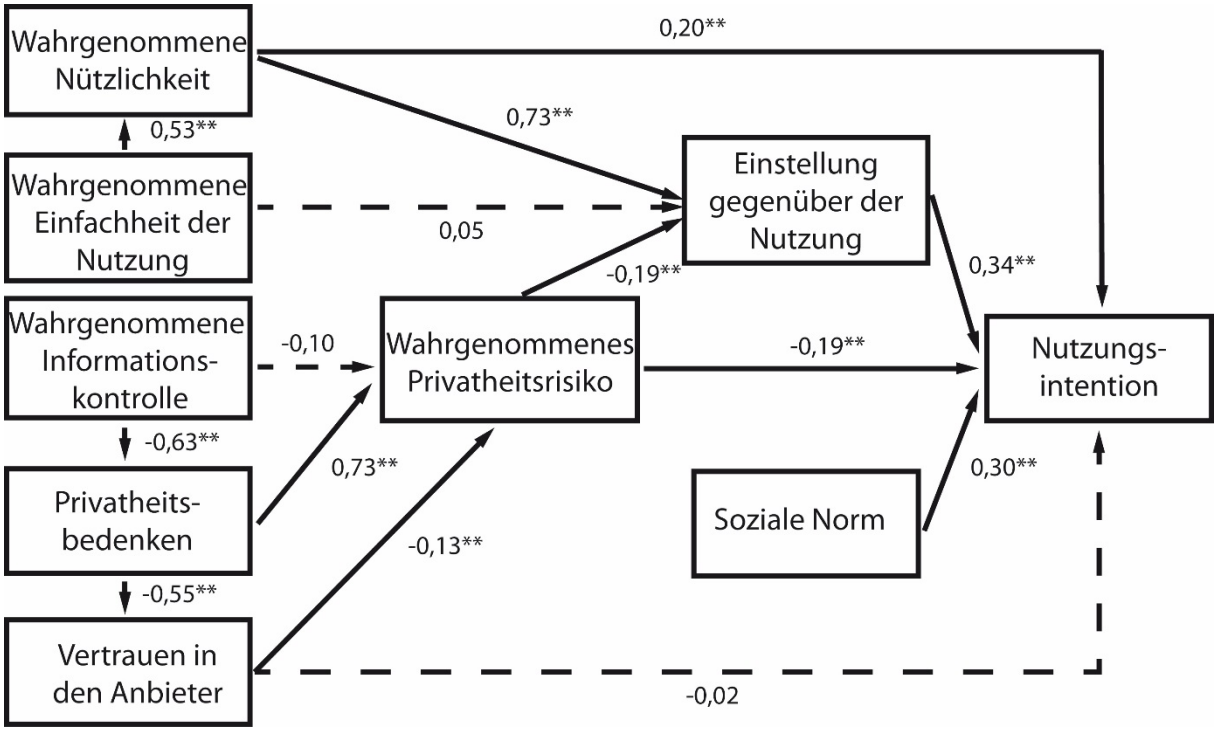


Abbildung A3: Strukturgleichungsmodell für sicherheitsbezogene vernetzte Mehrwertdienste im Automobil auf Basis der bereits in den Studien 1 und 2 verwendeten Skala für die wahrgenommene Nützlichkeit. Gestrichelte Linien kennzeichnen nicht-signifikante Pfadbeziehungen.

Anhang 15: Ergebnisse des Strukturgleichungsmodells für die Stichprobe mit expliziter Anzeige der datenempfangenden Partei (N = 90)

Tabelle A12. Ergebnisse der Berechnung des Strukturgleichungsmodells auf Basis der Teilnehmenden in Studie 3, die einen expliziten Hinweis auf die datenempfangende Partei angezeigt bekommen haben (N = 90).

Hypothese	*Beziehung*	β	t	p	
H 1.1	PU → ATT	0,68	10,42	< .001	H_0 abgelehnt
H 1.2	PU → BI	0,18	2,06	< .05	H_0 abgelehnt
H 1.3	PEOU → PU	0,56	5,85	< .001	H_0 abgelehnt
H 1.4	PEOU → ATT	0,03	0,48	> .05	H_0 nicht abgelehnt
H 1.5	ATT → BI	0,60	5,15	< .001	H_0 abgelehnt
H 1.6	SN → BI	0,12	2,09	< .05	H_0 abgelehnt
H 1.7	PC → PR	0,76	14,03	< .001	H_0 abgelehnt
H 1.8	PC → TR	-0,54	7,41	< .001	H_0 abgelehnt
H 1.9	TR → BI	0,05	0,77	> .05	H_0 nicht abgelehnt
H 1.10	TR → PR	-0,10	1,60	> .05	H_0 nicht abgelehnt
H 1.11	PR → BI	-0,08	1,45	> .05	H_0 nicht abgelehnt
H 1.12	PR → ATT	-0,27	4,17	< .001	H_0 abgelehnt
H 1.13	IC → PR	-0,12	1,47	> .05	H_0 nicht abgelehnt
H 1.14	IC → PC	-0,54	5,62	< .001	H_0 abgelehnt

Hinweis: Signifikanzniveau ist α = .05. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.

Anhang 16: Ergebnisse des Strukturgleichungsmodells für die Stichprobe ohne explizite Anzeige der datenempfangenden Partei (N = 109)

Tabelle A13. Ergebnisse der Berechnung des Strukturgleichungsmodells auf Basis der Teilnehmenden in Studie 3, die keinen expliziten Hinweis auf die datenempfangende Partei angezeigt bekommen haben (N = 109).

Hypothese	*Beziehung*	*β*	*t*	*p*	
H 1.1	PU → ATT	0,69	11,99	< .001	H_0 abgelehnt
H 1.2	PU → BI	0,13	1,47	> .05	H_0 nicht abgelehnt
H 1.3	PEOU → PU	0,47	5,84	< .001	H_0 abgelehnt
H 1.4	PEOU → ATT	0,10	5,84	< .001	H_0 abgelehnt
H 1.5	ATT → BI	0,51	5,10	< .001	H_0 abgelehnt
H 1.6	SN → BI	0,34	3,65	< .001	H_0 abgelehnt
H 1.7	PC → PR	0,74	9,12	< .001	H_0 abgelehnt
H 1.8	PC → TR	-0,57	9,03	< .001	H_0 abgelehnt
H 1.9	TR → BI	-0,10	1,78	> .05	H_0 nicht abgelehnt
H 1.10	TR → PR	-0,16	2,30	< .05	H_0 abgelehnt
H 1.11	PR → BI	-0,11	2,15	< .05	H_0 abgelehnt
H 1.12	PR → ATT	-0,21	4,19	< .001	H_0 abgelehnt
H 1.13	IC → PR	-0,04	0,52	> .05	H_0 nicht abgelehnt
H 1.14	IC → PC	-0,72	14,67	< .001	H_0 abgelehnt

Hinweis: Signifikanzniveau ist α = .05. IC = Wahrgenommene Privatheitskontrolle; TR = Vertrauen in den Anbieter; PC = Privatheitsbedenken; PR = Wahrgenommenes Privatheitsrisiko; SN = Soziale Norm; PU = Wahrgenommene Nützlichkeit; PEOU = Wahrgenommene Einfachheit der Nutzung; ATT = Einstellung gegenüber der Nutzung; BI = Nutzungsintention.